
แจ้งเตือนและข้อแนะนำ

# CYBER THREAT ALERTS

# 2012

โดย

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

แจ้งเตือนและข้อแนะนำ

# CYBER THREAT ALERTS 2012

โดย

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

# บทความ CYBER THREAT ALERTS 2012 โดย ThaiCERT


**ชื่อเรื่อง** บทความ CYBER THREAT ALERTS 2012 โดย ThaiCERT

**เรียบเรียงโดย** ทีมไทยเซิร์ต

**เลข ISBN** 978-974-9765-43-2

**พิมพ์ครั้งที่ 1** มกราคม 2556
**พิมพ์จำนวน** 500 เล่ม
**ราคา** 150 บาท



สงวนลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537


## จัดพิมพ์และเผยแพร่โดย


ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. เลขที่ 120 หมู่ 3 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

โทรศัพท์ 0-2142-2483

โทรสาร 0-2143-8071

เว็บไซต์ไทยเซิร์ต www.thaicert.or.th

เว็บไซต์ สพธอ. www.etda.or.th

เว็บไซต์กระทรวงฯ www.mict.go.th

# คำนำ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต ได้เริ่มดำเนินการภายใต้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร มาตั้งแต่วันที่ 1 กรกฎาคม พ.ศ. 2554 โดยให้บริการรับมือ วิเคราะห์ และดำเนินการประสานงานเพื่อแก้ไขปัญหาภัยคุกคามด้านสารสนเทศ

ไทยเซิร์ตมีพันธกิจเชิงรุกในการเพิ่มขีดความสามารถของทรัพยากรบุคคลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และมีกิจกรรมสร้างความตระหนักและพัฒนาทักษะความรู้ต่างๆ เช่น การซักซ้อมรับมือภัยคุกคามด้านสารสนเทศ และการแลกเปลี่ยนและเผยแพร่ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามด้านสารสนเทศ

หนังสือเล่มนี้เป็นรวบรวมบทความประเภทแจ้งเตือนและข้อแนะนำที่ได้เผยแพร่ผ่านเว็บไซต์ของไทยเซิร์ต (www.thaicert.or.th) ในช่วงระยะเวลาวันที่ 1 ธันวาคม 2554 - 31 ธันวาคม พ.ศ. 2555 ซึ่งทีมไทยเซิร์ตได้ติดตามข่าวสารจากแหล่งข่าวด้านความมั่นคงปลอดภัยระบบคอมพิวเตอร์ต่าง ๆ ทั่วโลก และกลั่นกรองเหตุการณ์ที่อาจส่งผลกระทบต่อคนไทยมาเผยแพร่ จึงทำให้บทความประเภทการแจ้งเตือนและข้อแนะนำนั้นมีเนื้อหาที่หลากหลาย เช่น การแจ้งเตือนช่องโหว่ของโปรแกรมที่มีการใช้งานอย่างแพร่หลายในประเทศไทย ไม่ว่าจะเป็นโปรแกรมจากบริษัท Adobe หรือโปรแกรมต่าง ๆ ที่ติดตั้งในระบบปฏิบัติการ Windows การแจ้งเตือนจากเหตุการณ์ที่อาจส่งผลกระทบต่อคนไทย เช่น เหตุการณ์ที่เว็บไซต์ Social Media ชื่อดังอย่าง LinkedIn ซึ่งมีคนไทยเป็นสมาชิกอยู่กว่า 250,000 คน ถูกแฮ็ก ทำให้รหัสผ่านของบัญชีผู้ใช้หลุดออกมากว่า 6.5 ล้านบัญชี เป็นต้น ดังนั้นผู้จัดทำจึงหวังเป็นอย่างยิ่งว่าหนังสือเล่มนี้ จะมีส่วนช่วยในการสร้างภูมิคุ้มกันให้กับสังคมออนไลน์ของประเทศไทย

สุรางคณา วายุภาพ

ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

# สารบัญ

# สารบัญรูป


# 1. ระวังภัย ช่องโหว่ 0-day ใน Adobe Reader และ Adobe Acrobat (CVE-2011-2462)

**วันที่ประกาศ** : 7 ธันวาคม 2554
**ปรับปรุงล่าสุด** : 8 ธันวาคม 2554
**เรื่อง** : ระวังภัยช่องโหว่ 0-day ใน Adobe Reader และ Adobe Acrobat (CVE-2011-2462)
**ประเภทภัยคุกคาม** : Intrusion

## ข้อมูลทั่วไป

Adobe แจ้งเตือนเมื่อวันที่ 6 ธันวาคม 2554 เรื่องช่องโหว่ 0-day รหัส CVE-2011-2462 โดยช่องโหว่ดังกล่าวมีผลกับซอฟต์แวร์ Adobe Reader 9.x, Adobe Reader X, Adobe Acrobat 9.x และ Adobe Acrobat X ซึ่งทาง Adobe แจ้งว่ามีการโจมตีผู้ใช้โปรแกรม Adobe Reader เวอร์ชัน 9.x บน Windows ผ่านช่องโหว่ดังกล่าวแล้ว

## ผลกระทบ

Adobe รายงานว่า ช่องโหว่ที่เกิดขึ้นคือ U3D memory corruption โดย U3D ย่อมาจาก Universal 3D ซึ่งเป็นไฟล์บีบอัด (Compressed file) ของไฟล์ภาพกราฟิก 3 มิติ ที่นิยมใช้ในหลายบริษัท เช่น Adobe, Intel หรือ Hewlett-Packard ผู้โจมตีจะส่งอีเมลโดยแนบไฟล์ PDF ที่ใส่โค้ดอันตรายลงไปในส่วน U3D หลังจากผู้รับเปิดไฟล์ดังกล่าว โค้ดอันตรายที่ฝังอยู่ในไฟล์ PDF จะเริ่มทำงาน หลังจากนั้นโปรแกรมจะ Crash และเปิดโอกาสให้ผู้โจมตีสามารถส่งคำสั่งเข้ามาควบคุมเครื่องคอมพิวเตอร์ของ เหยื่อได้

## ระบบที่ได้รับผลกระทบ

- Adobe Reader X (10.1.1) และเวอร์ชันต่ำกว่า 10.x สำหรับ Windows และ Macintosh
- Adobe Reader 9.4.6 และเวอร์ชันต่ำกว่า 9.x สำหรับ Windows, Macintosh และ UNIX
- Adobe Acrobat X (10.1.1) และเวอร์ชันต่ำกว่า 10.x สำหรับ Windows และ Macintosh
- Adobe Acrobat 9.4.6 และเวอร์ชันต่ำกว่า 9.x สำหรับ Windows และ Macintosh

หมายเหตุ : ช่องโหว่นี้ไม่มีผลกระทบต่อ Adobe Reader ใน Android และ Adobe Flash Player

## วิธีแก้ไข

ปัจจุบันยังไม่มีแพทช์สำหรับแก้ปัญหาช่องโหว่ดังกล่าว โดยทาง Adobe แจ้งว่า จะออกแพทช์ชั่วคราวสำหรับ Adobe Reader 9.x และ Acrobat 9.x สำหรับ Windows ภายในช่วงสัปดาห์ของวันที่ 12 ธันวาคม 2554 เนื่องจากโปรแกรม Adobe Reader X มีระบบ Protected Mode และ Adobe Acrobat X มีระบบ Protected View ซึ่งช่วยป้องกันการโจมตีโดยใช้ช่องโหว่ดังกล่าวได้อยู่แล้ว และทาง Adobe จะปล่อยซอฟต์แวร์ Adobe Reader 9.x, Adobe Reader X, Adobe Acrobat 9.x และ Adobe Acrobat X เวอร์ชันใหม่ ภายในวันที่ 10 มกราคม 2555

สำหรับผู้ที่ใช้งานโปรแกรม Adobe Reader X จะเปิดการทำงานของระบบ Protected Mode เพื่อป้องกันปัญหานี้อยู่แล้ว ผู้ใช้สามารถตรวจสอบการทำงานของระบบนี้ได้ด้วยการ

1. คลิกที่เมนู Edit > Preferences > General
2. ตรวจสอบว่าหัวข้อ “Enable Protected Mode at startup” ได้ถูกเลือกอยู่

สำหรับผู้ที่ใช้งานโปรแกรม Adobe Acrobat X จะเปิดการทำงานของระบบ Protected View เพื่อป้องกันปัญหานี้อยู่แล้ว ผู้ใช้สามารถตรวจสอบการทำงานของระบบนี้ได้ด้วยการ

1. คลิกที่เมนู Edit > Preferences > Security (Enhanced)
2. ตรวจสอบว่าหัวข้อ “Files from potentially unsafe locations” หรือ “All files” ถูกกำหนดไว้เป็น “Enable Enhanced Security”

อย่างไรก็ตาม ระหว่างที่ยังไม่มีการแก้ไขปัญหาอย่างเป็นทางการจาก Adobe ผู้ที่ใช้ซอฟต์แวร์ Adobe Reader 9.x หรือ Adobe Acrobat 9.x ควรเปลี่ยนมาใช้ซอฟต์แวร์ Adobe Reader X และ Adobe Acrobat X โดยเร็วที่สุด

## อ้างอิง


[4-1] http://www.adobe.com/support/security/advisories/apsa11-04.html

[4-2] http://blogs.adobe.com/asset/2011/12/background-on-cve-2011-2462.html

[4-3] http://osvdb.org/show/osvdb/77529

[4-4] http://www.computerworld.com/s/article/9222454/Hackers_exploit_Adobe_Reader_zero_day_may_be_targeting_defense_contractors


# 2. ระวังภัย ช่องโหว่ Serv-U File Server ทำให้ผู้ใช้เข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

**วันที่ประกาศ** : 7 ธันวาคม 2554
**ปรับปรุงล่าสุด** : 7 ธันวาคม 2554
**เรื่อง** : ระวังภัย ช่องโหว่ Serv-U File Server ทำให้ผู้ใช้เข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
**ประเภทภัยคุกคาม** : Intrusion

## ข้อมูลทั่วไป

โปรแกรม Serv-U File Server เป็นโปรแกรมที่ให้บริการ FTP Server ซึ่งรองรับระบบปฏิบัติการ Windows และ Linux ทั้งเวอร์ชัน 32 bit และ 64 bit โดยเมื่อวันที่ 1 ธันวาคม 2554 มีรายงานว่ามีการค้นพบช่องโหว่ของโปรแกรม Serv-U File Server ที่อนุญาตให้ผู้ใช้สามารถเข้าถึงไดเรกทอรีที่ปกติแล้วจะไม่สามารถเข้าถึงได้ โดยลักษณะของการโจมตี ผู้โจมตีจะล็อกอินด้วยบัญชีผู้ใช้ (Account) ของระบบ หรือ บัญชีผู้ใช้ที่เปิดให้ใช้งานได้โดยไม่ต้องกรอกรหัสผ่าน เช่น anonymous หรือ ftp จากนั้นจะอาศัยช่องโหว่ของการระบุที่อยู่ของไดเรกทอรี โดยใส่ค่าอักขระที่เป็นข้อยกเว้น ซึ่งไม่ได้มีการป้องกัน ทำให้ผู้โจมตีสามารถส่งคำสั่งไปยังตำแหน่งไดเรกทอรีอื่นๆ นอกเหนือส่วนที่ถูกจำกัดสิทธิในการเข้าถึงได้

## ผลกระทบ

ผู้โจมตีสามารถโจรกรรมหรือดาวน์โหลดข้อมูลต่างๆ ที่อยู่บนระบบออกมายังเครื่องคอมพิวเตอร์ของผู้โจมตี นอกจากนี้ยังอาจเปลี่ยนแปลง ลบ หรืออัปโหลดไวรัส, ม้าโทรจัน หรือข้อมูลที่เป็นอันตรายอื่นๆ เข้าไปยังเครื่องที่ให้บริการ FTP ได้

## ระบบที่ได้รับผลกระทบ

Serv-U File Server เวอร์ชันต่ำกว่า 11.1.0.5

## วิธีแก้ไข

ติดตั้งโปรแกรม Serv-U File Server เวอร์ชัน 11.1.0.5 ขึ้นไป

## อ้างอิง


[5-1] http://www.exploit-db.com/exploits/18182/

[5-2] http://www.serv-u.com/releasenotes/


# 3. ระวังภัย ช่องโหว่ 0-day ใน Adobe Flash Player (CVE-2011-4693, CVE-2011-4694)

**วันที่ประกาศ:** 16 ธันวาคม 2554
**ปรับปรุงล่าสุด:** 16 ธันวาคม 2554
**เรื่อง:** ระวังภัย ช่องโหว่ 0-day ใน Adobe Flash Player (CVE-2011-4693, CVE-2011-4694)
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

บริษัทวิจัยด้านความมั่นคงปลอดภัยซอฟต์แวร์คอมพิวเตอร์ชื่อ Intevydis ได้เผยแพร่วิดีโอสาธิตวิธีการโจมตีเครื่องคอมพิวเตอร์ที่ติดตั้งซอฟต์แวร์ Adobe Flash Player บนระบบปฏิบัติการ Windows [6-1] ซึ่งการโจมตีดังกล่าวใช้ช่องโหว่ที่ไม่เคยค้นพบและยังไม่มีวิธีแก้ไข (0-day) แต่เนื่องจากความน่าเชื่อถือของช่องโหว่ที่ค้นพบ ทำให้มีการออกเป็นหมายเลข CVE ขึ้นมาเพื่อการติดตามช่องโหว่ดังกล่าว คือ CVE-2011-4693 [6-2] และ CVE-2011-4694 [6-3] โดยระบุถึงลักษณะการโจมตีผ่านการเรียกไฟล์ SWF (Shockwave Flash) เพื่อเข้าควบคุมเครื่องคอมพิวเตอร์จากระยะไกล มีผลกับซอฟต์แวร์ Adobe Flash Player เวอร์ชัน 11.1.102.55 หรือต่ำกว่า บนระบบปฏิบัติการ Windows และ OS X [6-4] ปัจจุบัน Adobe ยังไม่มีแถลงการณ์เกี่ยวกับช่องโหว่นี้ [6-5]

## ผลกระทบ

ระบบที่เปิดไฟล์ SWF ที่โจมตีผ่านช่องโหว่ดังกล่าว จะเปิดโอกาสให้ผู้โจมตีสามารถสั่งให้เครื่องคอมพิวเตอร์ประมวลผลคำสั่งไม่ พึงประสงค์ และสามารถควบคุมเครื่องคอมพิวเตอร์จากระยะไกลได้ [6-4]

## ระบบที่ได้รับผลกระทบ

Adobe Flash Player เวอร์ชัน 11.1.102.55 หรือต่ำกว่า ทั้งบนระบบปฏิบัติการ Windows และ Mac OS X [6-4]

## วิธีแก้ไข

เนื่องจากปัจจุบันยังไม่มีคำชี้แจงอย่างเป็นทางการจาก Adobe ในเรื่องของช่องโหว่ดังกล่าว ดังนั้นผู้ใช้งานควรระวังในการเปิดเว็บไซต์ที่ไม่น่าเชื่อถือ รวมถึงไม่เปิดไฟล์ SWF ที่น่าสงสัย และหากเป็นไปได้ควรปิดการใช้งานปลั๊กอิน Abobe Flash Player ในเบราว์เซอร์ก่อนชั่วคราว จนกว่าจะมีการปรับปรุงแก้ไขช่องโหว่นี้ [6-1]

สำหรับผู้ใช้ Internet Explorer สามารถปิดการใช้งาน Adobe Flash Player ได้ดังนี้

1. คลิกที่เมนู Tools จากนั้นคลิก Manage Add-ons
2. คลิกเลือก Shockwave Flash Object ในส่วนของ Adobe Systems Incorporated จากนั้นคลิกปุ่ม Disable

สำหรับผู้ใช้ Google Chrome สามารถปิดการใช้งาน Adobe Flash Player ได้ดังนี้

1. ในช่อง Address Bar พิมพ์ข้อความ about:plugins
2. ที่รายชื่อปลั๊กอิน Shockwave Flash คลิก Disable

สำหรับผู้ใช้ Mozilla Firefox สามารถปิดการใช้งาน Adobe Flash Player ได้ดังนี้

1. คลิกที่เมนู Tools จากนั้นคลิก Add-ons
2. คลิกที่แท็บ Plugins
3. ที่รายชื่อปลั๊กอิน Shockwave Flash คลิกปุ่ม Disable

## อ้างอิง


[6-1] http://www.computerworld.com/s/article/9222546/Two_zero_day_vulnerabilities_found_in_Flash_Player

[6-2] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4693

[6-3] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4694

[6-4] http://www.securitytracker.com/id/1026392

[6-5] http://reviews.cnet.com/8301-13727_7-57340665-263/new-zero-day-vulnerabilities-found-in-adobe-flash-player/




# 4. ระวังภัยการโจมตีผู้ใช้ Facebook ผ่านปลั๊กอินปลอมของ YouTube

**วันที่ประกาศ:** 9 ม.ค. 2555
**ปรับปรุงล่าสุด:** 9 ม.ค. 2555
**เรื่อง:** ระวังภัย การโจมตีผู้ใช้ Facebook ผ่านปลั๊กอินปลอมของ YouTube
**ประเภทภัยคุกคาม:** Malicious Code

## ข้อมูลทั่วไป

หลังจากวันที่ 1 มกราคม 2555 ผู้ใช้ Facebook หลายรายได้แจ้งเตือนว่ามีการโจมตีรูปแบบใหม่ ด้วยการหลอกให้คลิกเข้าไปยังลิงก์ของเว็บไซต์อันตราย เพื่อทำการติดตั้งส่วนเสริมของโปรแกรมเว็บเบราว์เซอร์ (ปลั๊กอิน) เมื่อผู้ใช้หลงกลติดตั้งปลั๊กอินดังกล่าว จะถูกสวมรอยโพสต์ลิงก์ของเว็บไซต์อันตรายลงในหน้ากระดานข่าว Facebook ของตนเอง รวมถึงหน้ากระดานข่าวอื่นๆ ที่ผู้ใช้คนนั้นเป็นสมาชิกอยู่ด้วย รูปแบบลิงก์และข้อความที่โพสต์จะมีลักษณะคล้ายกับรูปที่ 1 (1-1)

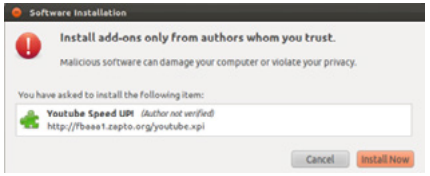

*รูปที่ 1. (1-1) ตัวอย่างการโพสต์ลิงก์ของเว็บไซต์อันตราย*

เว็บไซต์ที่อยู่ในลิงก์นั้น มีหน้าตาคล้ายกับเว็บไซต์ YouTube ดังรูปที่ 2 (1-2) และ 3 (1-3) พร้อมกับมีข้อความเชิญชวนให้ติดตั้งปลั๊กอินของ YouTube เช่น Youtube HD หรือ YouTube Speed UP! เพื่อดูคลิปวิดีโอในเว็บไซต์นั้น

*รูปที่ 2. (1-2) ตัวอย่างเว็บไซต์หลอกลวงของ YouTube เปิดโดย Google Chrome*


*รูปที่ 3. (1-3) ตัวอย่างเว็บไซต์หลอกลวงของ YouTube เปิดโดย Mozilla*

Firefoxซึ่งหากผู้ใช้ตรวจสอบรายละเอียดของปลั๊กอินดังกล่าว จะพบว่าปลั๊กอินที่จะติดตั้งไม่ได้มาจาก YouTube แต่อย่างใด โดยสังเกตได้จากข้อความ “Author not verified” ซึ่งเป็นการบอกว่า ไม่สามารถตรวจสอบผู้พัฒนาปลั๊กอินนี้ได้ รวมถึง URL ของปลั๊กอินก็มาจากเว็บไซต์ที่ไม่ใช่เว็บไซต์ทางการของผู้พัฒนาเบราว์เซอร์ ดังรูปที่ 4 (1-4)




*รูปที่ 4. (1-4) หน้าจอการติดตั้งปลั๊กอิน Youtube Speed UP*

## ผลกระทบ

หากผู้ใช้หลงกลติดตั้งปลั๊กอินจากเว็บไซต์ดังกล่าวแล้ว จะถูกส่งไปยังหน้าล็อกอินของ Facebook ดังรูปที่ 5 (1-5) ซึ่งหน้าล็อกอินที่พบนี้ ไม่ใช่การล็อกอินจากหน้าหลักของ Facebook แต่เป็นการล็อกอินผ่าน Application อีกทีหนึ่ง

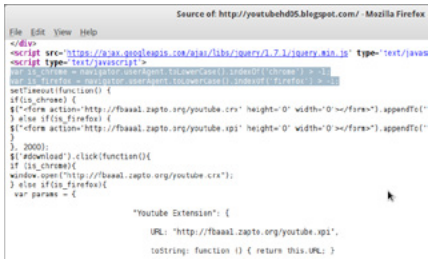

*รูปที่ 5. (1-5) หน้าจอล็อกอินของ Facebook ผ่าน Application ชื่อ Texas HoldEm Poker*

แต่หากผู้ใช้มีการล็อกอินเว็บไซต์ Facebook อยู่แล้ว ตัวปลั๊ก

อินของเบราว์เซอร์ ซึ่งจริงๆ แล้วเป็นโปรแกรมไม่พึงประสงค์ จะทำการโพสต์ลิงก์ของเว็บไซต์อันตรายดังกล่าวลงในหน้า Facebook ของผู้ใช้ เพื่อเผยแพร่ปลั๊กอินอันตรายนี้ให้กับบุคคลอื่นต่อไป

## ระบบที่ได้รับผลกระทบ

จากการตรวจสอบ Source Code ของเว็บไซต์ พบว่าปลั๊กอินดังกล่าวมีผลกระทบกับเบราว์เซอร์ Google Chrome และ Mozilla Firefox ทุกเวอร์ชัน ดังรูปที่ 6 (1-6)




*รูปที่ 6. (1-6) ตัวอย่าง Source Code จากหน้าเว็บไซต์*

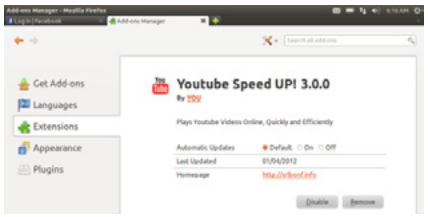
## ข้อแนะนำในการป้องกันและแก้ไข

หากผู้ใช้ถูกโจมตีด้วยวิธีดังกล่าว สามารถแก้ไขได้ดังนี้

1. ลบปลั๊กอิน YouTube HD หรือ YouTube Speed UP! ออกจากเบราว์เซอร์ ดังรูปที่ 7

   o วิธีการลบปลั๊กอินใน Google Chrome https://support.google.com/chrome/bin/answer.py?hl=th&answer=142064&p=cpn_plugins

   o วิธีการลบปลั๊กอินใน Mozilla Firefox http://support.mozilla.org/en-US/kb/Uninstalling%20add-ons




*รูปที่ 7.(1-7) ตัวอย่างการลบปลั๊กอิน YouTube Speed UP! ออกจากเบราว์เซอร์ Mozilla Firefox*

2. เปลี่ยนรหัสผ่านในการเข้าสู่ระบบของเว็บไซต์ Facebook
3. ทำการสแกนไวรัสในระบบ เพื่อกำจัดโปรแกรมไม่พึงประสงค์อื่นๆ ที่อาจติดมาด้วย

จะเห็นได้ว่า การโจมตีผ่านทาง Social Media ด้วยการหลอกให้ติดตั้งปลั๊กอินในเบราว์เซอร์นั้นเป็นตัวอย่างของภัยคุกคามรูปแบบใหม่ ที่มีแนวโน้มจะเพิ่มสูงขึ้นในอนาคต ไทยเซิร์ตมีข้อแนะนำในการใช้งาน Social Media ให้มีความมั่นคงปลอดภัย เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นในอนาคตได้ ดังนี้

1. ไม่คลิกลิงก์ที่ไม่น่าไว้วางใจ โดยเฉพาะลิงก์ของเว็บไซต์ที่ให้บริการย่อ URL
2. ไม่ติดตั้งโปรแกรม หรือปลั๊กอินของเบราว์เซอร์จากแหล่งที่มาที่ไม่น่าเชื่อถือ ถ้าเป็นไปได้ควรติดตั้งเฉพาะปลั๊กอินที่มีจากแหล่งดาวน์โหลดของผู้ผลิต เบราว์เซอร์เท่านั้น เช่น Chrome Web Store (https://chrome.google.com/webstore) ของ Google Chrome หรือ Mozilla Addon (https://addons.mozilla.org) ของ Mozilla Firefox
3. ในการเข้าสู่ระบบของบริการ Social Media ควรเข้าสู่ระบบด้วยการพิมพ์ URL ของเว็บไซต์ในช่อง Address bar ด้วยตนเองเท่านั้น



# 5. ระวังภัย ช่องโหว่ระดับ Kernel ใน Windows 64 bit ทำให้เกิด Memory Corruption

**วันที่ประกาศ:** 9 มกราคม 2554
**ปรับปรุงล่าสุด:** 9 มกราคม 2554
**เรื่อง:** ระวังภัย ช่องโหว่ระดับ Kernel ใน Windows 64 bit ทำให้เกิด Memory Corruption
**ประเภทภัยคุกคาม:** Intrusion, DoS (Denial of Service)

## ข้อมูลทั่วไป

บริษัท Secunia ซึ่งวิจัยเกี่ยวกับความมั่นคงปลอดภัยทางระบบคอมพิวเตอร์ ได้แจ้งเตือนภัยคุกคามใหม่ที่พบในระบบปฏิบัติการ Windows 64 bit โจมตีผ่านช่องโหว่ในไฟล์ Kernel ของ Windows (win32k.sys) ทำให้เกิดการเรียกใช้หน่วยความจำผิดพลาด (Memory Corruption) ส่งผลให้ผู้โจมตีสามารถสั่งประมวลผลโค้ดอันตรายโดยได้ระดับสิทธิของผู้ดูแลระบบ (Administrator) หรือทำให้เกิด Blue Screen of Death ได้ [7-1]

ช่องโหว่ดังกล่าวเกิดจากระบบที่ใช้ในการวาดส่วนติดต่อผู้ใช้ (User Interface) ของ Windows ไม่สามารถรองรับการวาดส่วนติดต่อที่มีขนาดความสูงมากๆ ได้ [7-2] นักวิจัยทดลองการโจมตีผ่านช่องโหว่นี้ด้วยการสร้างหน้าเว็บที่มีส่วนควบคุม ที่สามารถกำหนดค่า “height” ได้ เช่น iframe แล้วกำหนดค่า “height” เป็นตัวเลขจำนวนมาก ทำให้เมื่อใช้เบราว์เซอร์เปิดเว็บไซต์ดังกล่าว ระบบจะไม่สามารถทำงานต่อได้ [7-3] [7-4] ช่องโหว่ที่พบนี้มีผลกับทุกเบราว์เซอร์ที่ใช้ฟังก์ชั่นของ Windows ในการวาดส่วนติดต่อผู้ใช้ [7-5] [7-6]

## ผลกระทบ

หากผู้ใช้ Windows 64 bit เปิดเว็บไซต์ที่มีโค้ดดังกล่าวอยู่ จะทำให้ผู้โจมตีสามารถสั่งประมวลผลโค้ดอันตรายหรือทำให้เครื่องของผู้ใช้ไม่สามารถทำงานต่อได้

## ระบบที่ได้รับผลกระทบ

ทุกเบราว์เซอร์บนระบบปฏิบัติการ Windows XP/Vista/7/8 เวอร์ชัน 64 bit ที่ใช้ฟังก์ชั่นของระบบในการวาดส่วนประกอบบนหน้าเว็บ เช่น

- Microsoft Internet Explorer เวอร์ชันต่ำกว่า 9.0
- Apple Safari ทุกเวอร์ชัน
- Google Chrome ทุกเวอร์ชัน
- Mozilla Firefox ทุกเวอร์ชัน

## ข้อแนะนำในการป้องกันและแก้ไข

Microsoft ยังไม่มีการประกาศข้อมูลเพิ่มเติมเกี่ยวกับช่องโหว่นี้ อย่างไรก็ตาม จากข้อมูลของผู้วิจัยช่องโหว่ดังกล่าว พบว่าไม่สามารถโจมตี Internet Explorer 9.0 ได้ เนื่องจากมี Engine ในการแสดงผลเป็นของตัวเอง ไม่ได้ใช้ฟังก์ชั่นของระบบในการวาดส่วนประกอบบนหน้าเว็บ นอกจากนี้ยังมีข้อมูลเพิ่มเติมว่าช่องโหว่ดังกล่าวนี้ไม่มีผลกระทบต่อผู้ใช้ที่ปรับแต่งรูปแบบ Theme ของ Windows เป็น Windows Classic [7-7]

## อ้างอิง

[7-1] http://secunia.com/advisories/47237

[7-2] http://pastebin.com/XTWnLF3p

[7-3] https://twitter.com/#!/w3bd3vil/status/148454992989261824

[7-4] http://www.youtube.com/watch?v=u-62ZqrhD2k

[7-5] http://blog.romidar.com/2011/12/windows-7-x64-safari-0-day-vulnerability/

[7-6] http://thehackernews.com/2011/12/windows-7-64-bit-memory-corruption.html

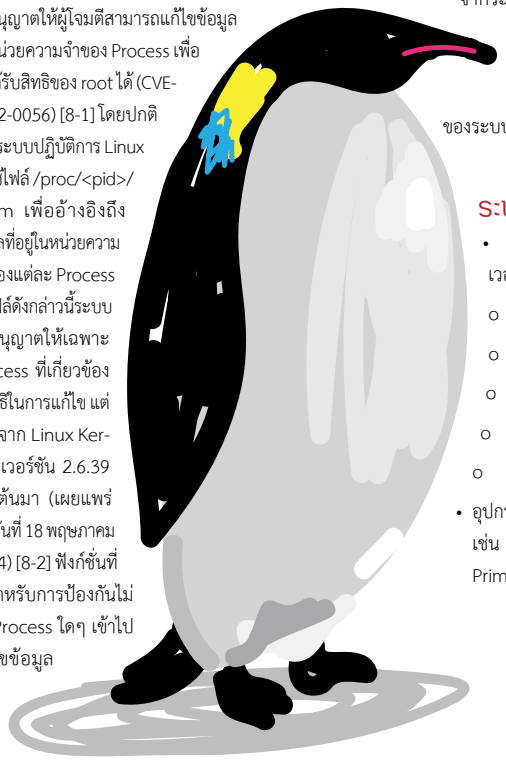
[7-7] https://twitter.com/#!/aionescu/status/149773613426425856

# 6. ระวังภัย ช่องโหว่ใน Linux Kernel 2.6.39 เป็นต้นไป ทำให้ผู้โจมตีได้สิทธิของ root

**วันที่ประกาศ:** 30 มกราคม 2555
**ปรับปรุงล่าสุด:** 30 มกราคม 2555
**เรื่อง:** ระวังภัย ช่องโหว่ใน Linux Kernel 2.6.39 เป็นต้นไป ทำให้ผู้โจมตีได้สิทธิของ root
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

ผู้เชี่ยวชาญได้แจ้งเตือนช่องโหว่ของ Linux Kernel ซึ่งอนุญาตให้ผู้โจมตีสามารถแก้ไขข้อมูลในหน่วยความจำของ Process เพื่อให้ได้รับสิทธิของ root ได้ (CVE-2012-0056) [8-1] โดยปกติแล้วระบบปฏิบัติการ Linux จะใช้ไฟล์ /proc/<pid>/mem เพื่ออ้างอิงถึงข้อมูลที่อยู่ในหน่วยความจำของแต่ละ Process ซึ่งไฟล์ดังกล่าวนี้ระบบจะอนุญาตให้เฉพาะ Process ที่เกี่ยวข้องมีสิทธิในการแก้ไข แต่หลังจาก Linux Kernel เวอร์ชัน 2.6.39 เป็นต้นมา (เผยแพร่เมื่อวันที่ 18 พฤษภาคม 2554) [8-2] ฟังก์ชั่นที่ใช้สำหรับการป้องกันไม่ให้ Process ใดๆ เข้าไปแก้ไขข้อมูลใน หน่วยความจำของ Process อื่นได้ถูกนำออกไป [8-3] นักวิจัยที่ค้นพบช่องโหว่นี้ได้พัฒนาซอฟต์แวร์เพื่อใช้ในการทดสอบสมมุติฐาน (Proof of Concept) ว่าช่องโหว่ดังกล่าวสามารถทำงานได้จริง โดยได้พัฒนาโปรแกรมเพื่อเข้าไปแก้ไขข้อมูลในหน่วยความจำของ Process su (Super User) เพื่อให้ผู้ใช้ทั่วไปได้รับสิทธิของ root [8-4] นอกจากนี้ยังพบว่าช่องโหว่ดังกล่าวมีผลกับอุปกรณ์ที่ติดตั้งระบบปฏิบัติการ Android เวอร์ชัน 4.0 อีกด้วย [8-5]



## ผลกระทบ

ผู้ใช้งานระบบปฏิบัติการ Linux ที่ติดตั้ง Kernel เวอร์ชัน 2.6.39 ถึง 3.2.1 มีความเสี่ยงที่จะถูกโจมตีจากผู้ไม่หวังดีเพื่อครอบครองสิทธิการเป็น root ของระบบได้ ตัวอย่างวีดีโอการโจมตีสามารถดูได้จาก http://www.youtube.com/watch?v=OKn-th3R9nI4

เนื่องจากระบบปฏิบัติการ Android ถูกพัฒนาโดยใช้พื้นฐานจากระบบปฏิบัติการ Linux ทำให้ระบบปฏิบัติการ Android เวอร์ชัน 4.0 ซึ่งใช้ Linux Kernel เวอร์ชัน 3 ได้รับผลกระทบไปด้วย โดยอาจมีผู้พัฒนาซอฟต์แวร์เพื่อให้ได้รับสิทธิเป็นของ root ของระบบได้

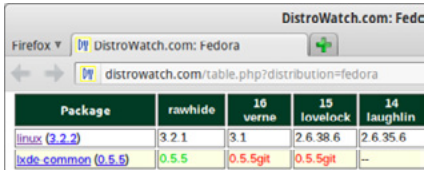
## ระบบที่ได้รับผลกระทบ

- ระบบปฏิบัติการ Linux ที่ติดตั้ง Kernel ตั้งแต่เวอร์ชัน 2.6.39 ถึง 3.2.1 เช่น
  - Ubuntu 11.10
  - Red Hat Enterprise Linux 6
  - Fedora 16
  - openSUSE 12.1
  - Debian wheezy (รุ่นทดสอบของเวอร์ชัน 7)
- อุปกรณ์ที่ติดตั้งระบบปฏิบัติการ Android เวอร์ชัน 4.0 เช่น Galaxy Nexus, Galaxy S และ Transformer Prime เป็นต้น



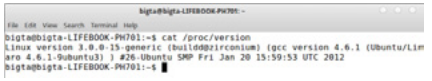
## วิธีการตรวจสอบเวอร์ชันของ Kernel

1. หากผู้ใช้งานระบบปฏิบัติการ Linux ต้องการตรวจสอบเวอร์ชันของ Kernel ที่มากับ Distribution ที่ตนเองใช้อยู่ว่าได้รับผลกระทบหรือไม่ สามารถตรวจสอบได้ด้วยการเข้าไปที่เว็บไซต์ http://www.distrowatch.com เลือก Distribution ที่ต้องการตรวจสอบ จากนั้นดูในส่วนของ Package ที่ชื่อ linux ตัวอย่างการตรวจสอบเวอร์ชันของ Kernel ของระบบปฏิบัติการ Fedora 16 พบว่าใช้ Kernel เวอร์ชัน 3.1 ดังรูปที่ 11 (8-1)




*รูปที่ 8.ตัวอย่างการตรวจสอบเวอร์ชันของ Kernel ของระบบปฏิบัติการ Fedo*

2. สำหรับการตรวจสอบเวอร์ชันของ Kernel ที่ใช้งานอยู่ในปัจจุบัน เนื่องจากวิธีการตรวจสอบเวอร์ชันของ Kernel ของระบบปฏิบัติการ Linux นั้นอาจแตกต่างกันไปตามแต่ละ Distribution ผู้ใช้งานระบบปฏิบัติการ Linux สามารถตรวจสอบเวอร์ชันของ Kernel ที่ตนเองใช้อยู่ได้ตามวิธีในเว็บไซต์ CyberCiti.biz ตัวอย่างการตรวจสอบเวอร์ชันของ Kernel ของระบบปฏิบัติการ Ubuntu เป็นดังรูปที่




*รูปที่ 9. (8-2) ตัวอย่างการตรวจสอบเวอร์ชันของ Kernel ของระบบปฏิบัติการ Ubuntu*

## ข้อแนะนำในการป้องกันและแก้ไข

ทาง Kernel.org ได้ปรับปรุงแก้ไขช่องโหว่ดังกล่าวเมื่อวันที่ 17 มกราคม 2555 [8-6] และการแก้ไขนี้จะมีผลตั้งแต่ Linux Kernel 3.2.2 เป็นต้นไป [8-7] ทางผู้พัฒนาระบบปฏิบัติการ Linux Distribution ต่างๆ เช่น Ubuntu, Debian หรือ Red Hat ได้นำ Patch จาก Kernel.org ไปปรับปรุงใน Kernel ของตนเอง และได้ทำการเผยแพร่ Kernel เวอร์ชันใหม่ที่แก้ไขปัญหาดังกล่าว ผ่านช่องทางการอัพเดทของแต่ละ Distribution แล้ว [8-8] [8-9] ซึ่งเวอร์ชันของ Kernel ที่ถูกปรับปรุงช่องโหว่ดังกล่าวอาจแตกต่างกันไปตามแต่ละ Distribution ผู้ใช้งานควรตรวจสอบการอัพเดทและปรับปรุงระบบให้เป็น Kernel เวอร์ชันที่ถูกปรับปรุงหลังจากวันที่ 17 มกราคม 2555 โดยเร็วที่สุด

## อ้างอิง

[8-1] http://www.h-online.com/security/news/item/Linux-root-exploit-due-to-memory-access-Update-2-1419834.html

[8-2] https://lkml.org/lkml/2011/5/19/16

[8-3] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=198214a7

[8-4] http://blog.zx2c4.com/749

[8-5] https://github.com/saurik/mempodroid

[8-6] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=e268337dfe26df-c7efd422a804dbb27977a3cccc

[8-7] http://www.kernel.org/pub/linux/kernel/v3.0/ChangeLog-3.2.2

[8-8] https://lists.ubuntu.com/archives/ubuntu-security-announce/2012-January/001557.html

[8-9] https://www.redhat.com/security/data/cve/CVE-2012-0056.html

# 7. ระวังภัย Symantec ถูกแฮ็กเกอร์ขโมย Source code เตือนลูกค้าระวังการโจมตี 0-day

**วันที่ประกาศ:** 30 มกราคม 2555
**ปรับปรุงล่าสุด:** 30 มกราคม 2555
**เรื่อง:** ระวังภัย Symantec ถูกแฮ็กเกอร์ขโมย Source code เตือนลูกค้าระวังการโจมตี 0-day
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

เมื่อวันที่ 24 มกราคม 2555 บริษัท Symantec ผู้ผลิตซอฟต์แวร์ด้านความมั่นคงปลอดภัย ได้ประกาศผ่านหน้าเว็บไซต์ของตนว่า กลุ่มแฮ็กเกอร์ที่ใช้ชื่อ Anonymous สามารถเจาะเข้าระบบของ Symantec ได้สำเร็จและได้ทำการคัดลอกข้อมูล Source code ของโปรแกรมที่ถูกพัฒนาในปี พ.ศ. 2549 [9-1]

## ผลกระทบ

ในเบื้องต้น Symantec ยังไม่ได้ประกาศข้อมูลเวอร์ชันของซอฟต์แวร์ที่ถูกขโมย Source code ไป แต่อย่างไรก็ตาม Symantec ได้แนะนำว่าควรอัพเกรดซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุด เนื่องจากผู้ใช้งานซอฟต์แวร์ดังกล่าวอาจถูกโจมตีจากช่องโหว่ 0-day ได้

สำหรับผู้ที่ใช้โปรแกรม pcAnywhere ซึ่งเป็นโปรแกรมที่ใช้สำหรับเข้าถึงและควบคุมเครื่องคอมพิวเตอร์จากระยะไกล Symantec แจ้งว่ามีความเสี่ยงที่จะถูกผู้ไม่หวังดีโจมตีด้วยวิธี Man-in-the-middle รวมไปถึงการสั่งประมวลผลคำสั่งอันตรายจากระยะไกล (Remote execution) ได้

## ระบบที่ได้รับผลกระทบ

ซอฟต์แวร์ของ Symantec ที่ถูกพัฒนาในปี พ.ศ. 2549 (ค.ศ. 2006) ได้แก่

- Norton Antivirus Corporate Edition
- Norton Internet Security
- Norton SystemWorks (เฉพาะ Norton Utilities และ Norton GoBack)
- Symantec Endpoint Protection (SEP) 11.0
- Symantec Antivirus 10.2
- pcAnywhere

## ข้อแนะนำในการป้องกันและแก้ไข

บริษัท Symantec ได้แนะนำให้ผู้ที่ใช้งานซอฟต์แวร์ที่ได้รับผลกระทบ อัพเกรดซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุด เนื่องจากบางซอฟต์แวร์ที่ถูกขโมย Source code ไปนั้นได้สิ้นสุดการสนับสนุนทางเทคนิคแล้ว

สำหรับ ผู้ที่ใช้ซอฟต์แวร์ pcAnywhere ทาง Symantec ได้ออกโปรแกรม Hot fix เพื่อปรับปรุงแก้ไขช่องโหว่บางส่วนในเวอร์ชัน 12.5 (เวอร์ชันปัจจุบัน) แล้ว [9-2] อย่างไรก็ตาม ผู้ที่ได้ Source code ไป อาจพัฒนาเครื่องมือเพื่อใช้ในการโจมตีรูปแบบใหม่ได้ ดังนั้นจึงควรปิดการทำงานของโปรแกรม pcAnywhere และเปิดใช้งานในกรณีที่จำเป็นจริงๆ เท่านั้น [9-3]

## อ้างอิง


[9-1]http://www.symantec.com/theme.jsp?themeid=anonymous-code-claims&inid=us_ghp_banner1_anonymous

[9-2] http://www.symantec.com/connect/blogs/important-information-pcanywhere

[9-3] http://www.symantec.com/connect/sites/default/files/pcAnywhere%20Security%20Recommendations%20WP_01_23_Final.pdf



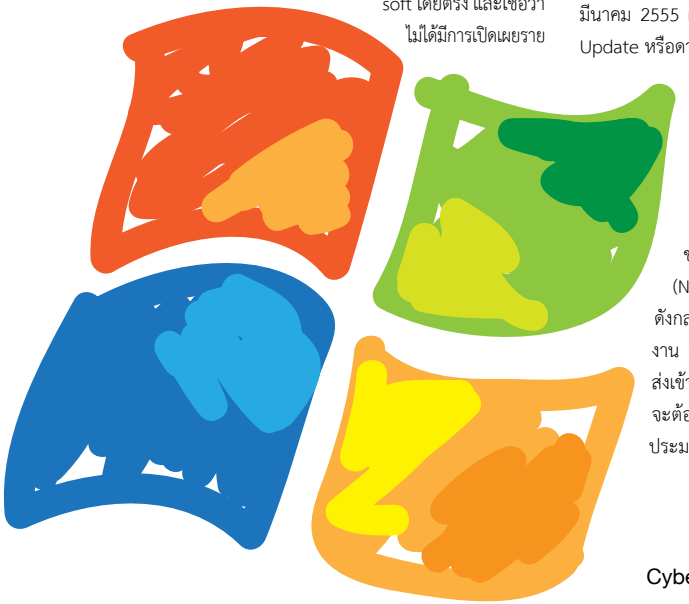

# 8. Microsoft เตือนผู้ใช้ Windows ติดตั้งแพทช์แก้ไขช่องโหว่ CVE-2012-0002 โดยด่วน

**วันที่ประกาศ:** 15 มีนาคม 2555
**ปรับปรุงล่าสุด:** 15 มีนาคม 2555
**เรื่อง:** Microsoft เตือนผู้ใช้ Windows ติดตั้งแพทช์แก้ไขช่องโหว่ CVE-2012-0002 โดยด่วน
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

Microsoft ได้ประกาศ Security Bulletin MS12-020 เพื่อแจ้งเตือนผู้ใช้งานระบบปฏิบัติการ Windows ทุกเวอร์ชัน ให้ทำการติดตั้งแพทช์ KB2621440 เพื่อแก้ไขปัญหาช่องโหว่ CVE-2012-0002 ซึ่งอนุญาตให้ผู้ไม่หวังดีส่งแพ็กเกจ RDP (Remote Desktop Protocol) เข้ามายังระบบ เพื่อสั่งให้ประมวลผลคำสั่งที่ไม่พึงประสงค์จากระยะไกลได้ (Remote Code Execution) [10-1]

อย่างไรก็ตาม ถึงแม้ว่าช่องโหว่ดังกล่าวได้ถูกแจ้งมายัง Microsoft โดยตรง และเชื่อว่าไม่ได้มีการเปิดเผยรายละเอียดของช่องโหว่นี้ออกสู่สาธารณะ แต่ทาง Microsoft ได้คาดการณ์ว่า ไฟล์แพทช์ KB2621440 ที่เผยแพร่ออกไป สามารถถูกผู้ไม่หวังดีทำการ Reverse engineering และเขียนโปรแกรมเพื่อใช้ในการโจมตีผ่านช่องโหว่นี้ได้ภายในเวลา 30 วัน ดังนั้นผู้ใช้งานระบบปฏิบัติการ Windows จึงควรติดตั้งแพทช์เพื่อแก้ไขปัญหาดังกล่าวนี้โดยเร็วที่สุด [10-2]



## ผลกระทบ

ผู้ใช้งานระบบปฏิบัติการ Windows ทุกเวอร์ชัน ที่เปิดใช้งานฟังก์ชั่น RDP (TCP Port 3389) มีโอกาสที่จะถูกโจมตีโดยผู้ไม่หวังดีได้

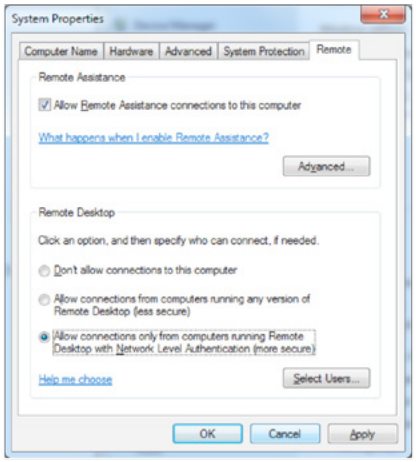
ระบบที่ได้รับผลกระทบ

- Windows XP Service Pack 3
- Windows Server 2003 Service Pack 2
- Windows Vista Service Pack 2
- Windows Server 2008 Service Pack 2
- Windows 7 Service Pack 1
- Windows Server 2008 R2 Service Pack 1

## ข้อแนะนำในการป้องกันและแก้ไข

Microsoft ได้เผยแพร่แพทช์ KB2621440 เมื่อวันอังคารที่ 13 มีนาคม 2555 ผู้ใช้งานสามารถติดตั้งได้ผ่านทาง Windows Update หรือดาวน์โหลดได้จาก เว็บไซต์ของ Microsoft

หากผู้ใช้ยังไม่ได้ติดตั้งแพทช์ดังกล่าว Microsoft ได้แนะนำให้ย้าย RDP listeners port ไปไว้ที่ Non-standard port เป็นการชั่วคราว [10-3] และสำหรับผู้ที่ใช้งาน Windows Vista หรือใหม่กว่า สามารถเปิดการทำงานของระบบ Network Level Authentication (NLA) [10-4] เพื่อช่วยลดผลกระทบจากปัญหาดังกล่าวได้ ดังรูปที่ เพราะในระบบที่เปิดการใช้งาน NLA ถึงแม้ว่าคำสั่งอันตรายจะยังสามารถถูกส่งเข้ามายังระบบได้ แต่อย่างน้อยผู้โจมตีก็จำเป็นที่จะต้อง Authenticate เข้าสู่ Server เพื่อสั่งให้ประมวลผลคำสั่งดังกล่าว




*รูปที่ 10. (10-1) แสดงการเปิดการทำงานของระบบ NLA ใน Windows 7*

## อ้างอิง


[10-1] http://technet.microsoft.com/en-us/security/bulletin/ms12-020

[10-2] http://blogs.technet.com/b/srd/archive/2012/03/13/cve-2012-0002-a-closer-look-at-ms12-020-s-critical-issue.aspx

[10-3] http://isc.sans.edu/diary.html?storyid=12781&rss

[10-4] http://technet.microsoft.com/en-us/library/cc732713.aspx


# 9. Oracle เผลอปล่อยโค้ดที่ใช้ทดสอบการ DoS โปรแกรม MySQL

**วันที่ประกาศ:** 18 เมษายน 2555
**ปรับปรุงล่าสุด:** 18 เมษายน 2555
**เรื่อง:** Oracle เผลอปล่อยโค้ดที่ใช้ทดสอบการ DoS โปรแกรม MySQL
**ประเภทภัยคุกคาม:** Denial of Service

## ข้อมูลทั่วไป

หลังจากที่บริษัท Oracle ได้เผยแพร่โปรแกรม MySQL เวอร์ชัน 5.5.22 และ 5.1.62 เมื่อวันที่ 21 มีนาคม 2555 ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยได้ค้นพบไฟล์ที่นักพัฒนาใช้ในการทดสอบ ช่องโหว่ของระบบ (Proof of concept) ซึ่งไฟล์ดังกล่าวได้หลุดออกมาพร้อมกับโปรแกรมอัพเดท [11-1] [11-2]

## ผลกระทบ

ไฟล์สคริปต์ mysql-test/suite/innodb/t/innodb_bug13510739.test เป็นไฟล์ที่นักพัฒนาใช้ในการทดสอบช่องโหว่ของระบบ ผู้โจมตีที่มีสิทธิเข้าถึงระบบของ MySQL จะสามารถสั่ง import ไฟล์สคริปต์ดังกล่าวเพื่อทำให้ระบบ MySQL ไม่สามารถทำงานต่อได้ (DoS) ตัวอย่างการโจมตีสามารถดูได้จาก http://youtu.be/RHgdUoXIDro

## ระบบที่ได้รับผลกระทบ

ช่องโหว่ดังกล่าวเป็นการโจมตีผ่าน Bug หมายเลข #13510739 และ #63775 ซึ่งถูกแก้ไขแล้วในโปรแกรม MySQL เวอร์ชัน 5.5.22 และ 5.1.62 [11-3] [11-4] ถึงแม้ว่าปัจจุบันยังไม่มีการเผยแพร่รายละเอียดของ Bug ดังกล่าว แต่ผู้ไม่หวังดีก็สามารถโจมตีผ่านช่องโหว่นี้ในระบบที่ติดตั้งโปรแกรม MySQL เวอร์ชันต่ำกว่า 5.5.22 หรือ 5.1.62 ได้

## ข้อแนะนำในการป้องกันและแก้ไข

ปัจจุบันบริษัท Oracle ยังไม่มีคำชี้แจงเกี่ยวกับกรณีดังกล่าว ผู้ดูแลระบบที่ติดตั้งโปรแกรม MySQL เวอร์ชันต่ำกว่า 5.5.22 หรือ 5.1.62 ควรทำการอัพเดทให้เป็นเวอร์ชันล่าสุด

## อ้างอิง


[11-1] http://www.h-online.com/security/news/item/Oracle-accidentally-release-MySQL-DoS-proof-of-concept-1526146.html

[11-2] http://eromang.zataz.com/2012/04/10/oracle-mysql-innodb-bugs-13510739-and-63775-dos-demo/

[11-3] http://dev.mysql.com/doc/refman/5.5/en/news-5-5-22.html

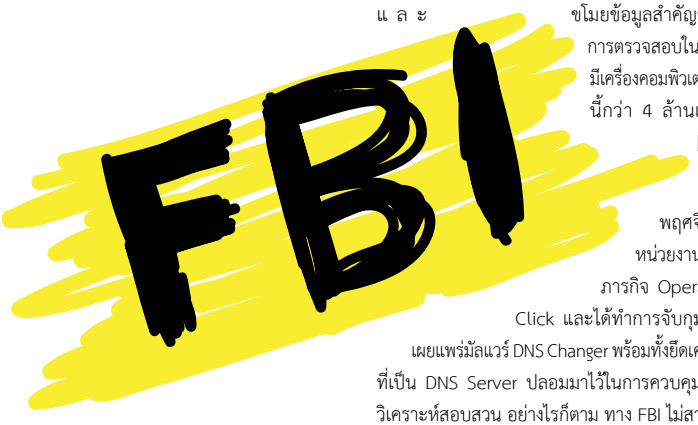
[11-4] http://dev.mysql.com/doc/refman/5.1/en/news-5-1-62.html


# 10. FBI เตรียมปิดเซิร์ฟเวอร์ DNS Changer ในวันที่ 9 ก.ค. 2555 เครื่องคอมพิวเตอร์ที่ติดมัลแวร์จะไม่สามารถใช้งานอินเทอร์เน็ตได้

**วันที่ประกาศ:** 27 เมษายน 2555
**ปรับปรุงล่าสุด:** 4 กรกฎาคม 2555
**เรื่อง:** FBI เตรียมปิดเซิร์ฟเวอร์ DNS Changer ในวันที่ 9 ก.ค. 2555 เครื่องคอมพิวเตอร์ที่ติดมัลแวร์จะไม่สามารถใช้งานอินเทอร์เน็ตได้
**ประเภทภัยคุกคาม:** Denial of Service

## ข้อมูลทั่วไป

มัลแวร์ DNS Changer ถูกค้นพบครั้งแรกเมื่อปี 2550 โดยสามารถทำงานได้ทั้งบนระบบปฏิบัติการ Windows และ Mac OS X มัลแวร์ดังกล่าวนี้จะเข้าไปเปลี่ยนแปลงการตั้งค่า DNS Server ในเครื่องที่ตกเป็นเหยื่อ เพื่อส่งผู้ใช้ไปยังเว็บไซต์หลอกลวงที่แฮ็กเกอร์สร้างขึ้น หรือติดตามการใช้งานอินเทอร์เน็ตและขโมยข้อมูลสำคัญของผู้ใช้ จากการตรวจสอบในตอนนั้นพบว่ามีเครื่องคอมพิวเตอร์ที่ติดมัลแวร์นี้กว่า 4 ล้านเครื่องทั่วโลก [12-1]




ในเดือนพฤศจิกายน 2554 หน่วยงาน FBI ได้ปฏิบัติภารกิจ Operation Ghost Click และได้ทำการจับกุมผู้พัฒนาและเผยแพร่มัลแวร์ DNS Changer พร้อมทั้งยึดเครื่องเซิร์ฟเวอร์ที่เป็น DNS Server ปลอมมาไว้ในการควบคุมเพื่อใช้ในการวิเคราะห์สอบสวน อย่างไรก็ตาม ทาง FBI ไม่สามารถที่จะปิดเซิร์ฟเวอร์ดังกล่าวได้ เนื่องจากเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ DNS Changer จำเป็นต้องติดต่อกับเครื่องเซิร์ฟเวอร์ที่เป็น

DNS Server ปลอมในทุกครั้งที่เชื่อมต่อกับอินเทอร์เน็ต หากปิดเซิร์ฟเวอร์ดังกล่าว จะทำให้เครื่องคอมพิวเตอร์เหล่านั้นถูกตัดขาดจากอินเทอร์เน็ตโดยทันที [12-2] [12-3]

FBI มีความพยายามที่จะปิดเครื่องเซิร์ฟเวอร์ดังกล่าวอยู่หลายครั้ง แต่ยังไม่สามารถทำได้เนื่องจากพบว่ามีคอมพิวเตอร์จำนวนมากที่ยังคงติดมัลแวร์ DNS Changer อยู่ โดยจากการตรวจสอบในเดือนมีนาคม 2555 พบว่าทั่วโลกยังมีเครื่องที่ติดมัลแวร์อยู่ประมาณ 450,000 เครื่อง และในจำนวนนั้นมีคอมพิวเตอร์ที่ใช้ในหน่วยงานสำคัญของทางราชการอยู่ด้วย จนกระทั่งวันที่ 23 เมษายน 2555 ทาง FBI ได้ประกาศว่า จะทำการปิดเครื่อง DNS Server ปลอมลงชั่วคราวในวันที่ 9 กรกฎาคม 2555 เพื่อทำความสะอาด การปิดเครื่องเซิร์ฟเวอร์ดังกล่าวอาจส่งผลให้เครื่องคอมพิวเตอร์ที่ยังติดมัลแวร์อยู่จะไม่สามารถเข้าใช้งานอินเทอร์เน็ตได้ [12-4] [12-5]

## ผลกระทบ

เครื่องคอมพิวเตอร์ที่ติดมัลแวร์ DNS Changer และไม่ได้ทำการแก้ไข จะไม่สามารถเข้าใช้งานอินเทอร์เน็ตได้ในวันที่ 9 กรกฎาคม 2555

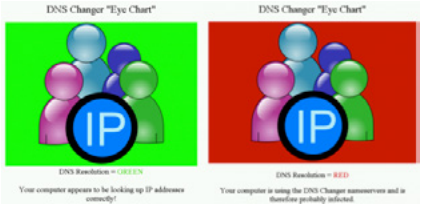
## ระบบที่ได้รับผลกระทบ

เครื่องคอมพิวเตอร์ที่ใช้งานระบบปฏิบัติการ Windows หรือ Mac OS X ที่ติดมัลแวร์ DNS Changer

## ข้อแนะนำในการป้องกันและแก้ไข

FBI ได้ประสานงานกับหน่วยงานต่างๆ ในการจัดทำเว็บไซต์ DNS Changer Working Group (DCWG) เพื่อช่วยตรวจสอบและกำจัดมัลแวร์ DNS Changer ออกจากระบบ ผู้ใช้สามารถเข้าไปใช้งานได้ที่ http://www.dcwg.org/

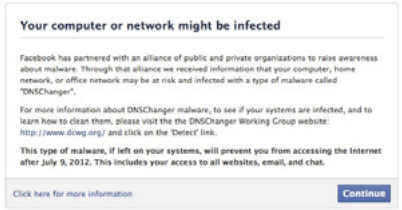
ในการตรวจสอบว่าเครื่องคอมพิวเตอร์ติดมัลแวร์หรือไม่ สามารถทำได้โดยการเข้าไปที่หน้า http://www.dcwg.org/detect/ แล้วคลิกที่ลิงก์ของเว็บไซต์ dns-ok จากนั้นเมื่อระบบทำการตรวจสอบเสร็จสิ้นก็จะแสดงข้อความเพื่อบอกว่าเครื่อง คอมพิวเตอร์ที่ใช้งานอยู่นั้นติดมัลแวร์หรือไม่ ถ้าหากไม่ติดก็จะแสดงข้อความ DNS Resolution = Green แต่หากติดมัลแวร์จะแสดงข้อความ DNS Resolution = Red ดังรูปที่ 14 (12-1)




*รูปที่ 11. 12-1) แสดงผลการตรวจสอบ DNS โดยใช้เว็บไซต์ www.dns-ok.us*

นอกจากนี้ ทาง Google และ Facebook ก็ได้ช่วยแจ้งเตือนผู้ใช้ที่ติดมัลแวร์ DSN Changer โดยหากทางเว็บไซต์ตรวจสอบได้ว่าผู้ใช้ติดมัลแวร์ ก็จะแสดงแถบข้อความแจ้งเตือนพร้อมทั้งแนะนำวิธีแก้ไขปัญหา ตัวอย่างการแจ้งเตือนเป็นดังรูปที่ และ [12-6] [12-7]


*รูปที่ 12. (12-2) การแจ้งเตือนผู้ใช้ที่ติดมัลแวร์ DNS Changer ของ Google*




*รูปที่ 13. (12-3) การแจ้งเตือนผู้ใช้ที่ติดมัลแวร์ DNS Changer ของ Facebook*

ซึ่งหากผู้ใช้ตรวจสอบแล้วพบว่าเครื่องติดมัลแวร์ DNS Changer ควรทำการกำจัดมัลแวร์ออกจากระบบโดยเร็วที่สุด สำหรับผู้ที่ใช้งานระบบปฏิบัติการ Windows ทาง Microsoft ได้แนะนำให้ดาวน์โหลดโปรแกรม Microsoft Malicious Software Removal Tool (MSRT) หรือ Microsoft Security Essentials มาใช้ในการกำจัดมัลแวร์ ส่วนผู้ที่ใช้งานระบบปฏิบัติการ Mac OS X สามารถดาวน์โหลดซอฟต์แวร์ DNSChanger Removal Tool จากเว็บไซต์ http://www.dnschanger.com/ มาใช้งานได้ฟรี

หลังจากกำจัดมัลแวร์แล้ว การตั้งค่า DNS Server ที่เกิดจากมัลแวร์อาจยังคงติดค้างอยู่ในระบบซึ่งอาจก่อให้เกิดปัญหาตามมาภายหลังได้ [12-8] ทาง Avira ได้พัฒนาเครื่องมือสำหรับซ่อมแซมระบบ Windows ที่ได้รับผลกระทบจากมัลแวร์ DNS Server โดยผู้ใช้สามารถดาวน์โหลดได้จากเว็บไซต์ของ Avira [12-9]

อย่างไรก็ตาม ผู้ใช้ควรติดตั้งซอฟต์แวร์แอนตี้ไวรัสและหมั่นอัพเดทฐานข้อมูลให้เป็นเวอร์ ชั่นล่าสุดอยู่เสมอ เพื่อช่วยในการตรวจจับและป้องกันปัญหาการติดมัลแวร์ที่อาจจะเกิดขึ้นได้ในอนาคต

## อ้างอิง


[12-1] http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

[12-2] http://reviews.cnet.com/8301-13727_7-57322316-263/fbi-tackles-dnschanger-malware-scam/

[12-3] http://www.fbi.gov/news/stories/2011/november/malware_110911

[12-4] http://www.theage.com.au/digital-life/consumer-security/internet-users-warned-of-big-black-out-in-july-20120329-1w172.html#ixzz1qW2sY-Ey8

[12-5] http://reviews.cnet.com/8301-13727_7-57421311-263/renewed-efforts-to-revert-dnschanger-in-effect

[12-6] http://nakedsecurity.sophos.com/2012/05/23/google-malware/

[12-7] https://www.facebook.com/notes/facebook-security/notifying-dnschanger-victims/10150833689760766

[12-8] https://www.hkcert.org/my_url/en/blog/12062701

[12-9] http://www.avira.com/en/support-for-home-knowledgebase-detail/kbid/1199


# 11. ช่องโหว่ TNS listener ใน Oracle Database (CVE-2012-1675)

**วันที่ประกาศ:** 3 พฤษภาคม 2555
**ปรับปรุงล่าสุด:** 3 พฤษภาคม 2555
**เรื่อง:** ช่องโหว่ TNS listener ใน Oracle Database (CVE-2012-1675)
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

TNS (Transparent Network Substrate) เป็นเทคโนโลยีที่ Oracle พัฒนาขึ้นมาเพื่อให้เครื่องคอมพิวเตอร์สามารถเชื่อมต่อเข้าสู่ระบบฐานข้อมูล ด้วยวิธี Peer-to-Peer โดยจะมี Service ชื่อ TNS listener เปิดพอร์ตที่ฝั่ง Database Server เพื่อรอรับการเชื่อมต่อจาก Client [13-1] [13-2] เทคโนโลยี TNS เริ่มมีใน Oracle Database Server ตั้งแต่เวอร์ชัน 8i ซึ่งถูกเผยแพร่ในปี 2542

ช่องโหว่ของ TNS Listener ถูกค้นพบและแจ้งไปยัง Oracle ตั้งแต่ปี 2551 [13-3] จนกระทั่งวันที่ 30 เมษายน 2555 Oracle ได้ออกประกาศแจ้งเตือนเรื่องความมั่นคงปลอดภัย (Security Alert) ของช่องโหว่ CVE-2012-1675 โดยได้เรียกช่องโหว่ดังกล่าวนี้ว่า “TNS Listener Poison Attack” [13-4]

## ผลกระทบ

ช่องโหว่ดังกล่าวอนุญาตให้ผู้โจมตีส่งคำสั่งเข้ามายัง Service ของ TNS listener เพื่อ Hijack Connection ของผู้ใช้ที่ล็อกอินอยู่ในระบบแล้ว โดยที่ผู้โจมตีไม่จำเป็นต้องใส่ Username หรือ Password แต่อย่างใด [13-5] [13-6] ตัวอย่างวิดีโอการโจมตีผ่านช่องโหว่นี้ดูได้จาก http://youtu.be/hE3-AkxSX3w

## ระบบที่ได้รับผลกระทบ

Oracle แจ้งในรายงาน Security Alert ว่ามีระบบที่ได้รับผลกระทบดังนี้ [13-4]

- Oracle Database 11g Release 2 เวอร์ชัน 11.2.0.2 และ 11.2.0.3
- Oracle Database 11g Release 1 เวอร์ชัน 11.1.0.7
- Oracle Database 10g Release 2 เวอร์ชัน 10.2.0.3, 10.2.0.4 และ 10.2.0.5
- เนื่องจาก Oracle Fusion Middleware, Oracle Enterprise Manager และ Oracle E-Business Suite มีส่วนการทำงานของ Oracle Database อยู่ในระบบ ทำให้ได้รับผลกระทบจากช่องโหว่ดังกล่าวด้วย

## ข้อแนะนำในการป้องกันและแก้ไข

Oracle ได้ปล่อยแพทช์ที่ใช้แก้ไขช่องโหว่นี้ผ่าน Critical Patch Update (CPU) ประจำเดือนเมษายน 2555 ซึ่งสามารถดาวน์โหลดได้จากเว็บไซต์ของ Oracle [13-7] อย่างไรก็ตาม แพทช์ดังกล่าวนี้แก้ไขช่องโหว่ในซอฟต์แวร์ Oracle Database Server เฉพาะเวอร์ชัน 10 และ 11 เท่านั้น เนื่องจากทาง Oracle ได้ให้เหตุผลว่า การปรับแต่งโค้ดเพื่อให้ใช้งานได้กับซอฟต์แวร์เวอร์ชันเก่านั้นเป็นเรื่องยากลำบากเพราะมีผลกระทบกับหลายส่วนของระบบ [13-8]

ผู้ที่ใช้งานซอฟต์แวร์ Oracle Database Server เวอร์ชันเก่าที่ไม่ได้รับการแพทช์ หากเป็นไปได้ควรอัพเกรดซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุด หรืออาจตั้งค่า Database Server ไม่ให้เครื่องที่ไม่เกี่ยวข้องเข้าใช้งาน TNS Service ได้ [13-9]

## อ้างอิง


[13-1] http://www.csee.umbc.edu/portal/help/oracle8/network.815/a67440/ch2.htm

[13-2] http://docs.oracle.com/cd/B10501_01/network.920/a96580/architec.htm

[13-3] http://seclists.org/fulldisclosure/2012/Apr/204

[13-4] http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html

[13-5] http://thehackernews.com/2012/05/oracle-database-new-zero-day-exploit.html

[13-6] http://www.joxeankoret.com/download/tnspoison.pdf

[13-7] http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html

[13-8] http://itknowledgeexchange.techtarget.com/security-bytes/oracle-trips-on-tns-zero-day-workaround/

[13-9] http://searchsecurity.techtarget.com/news/2240149475/Oracle-wont-patch-four-year-old-zero-day-in-TNS-listener




# 12. LinkedIn ถูกแฮ็ก รหัสผ่านหลุดกว่า 6.5 ล้านชื่อ

**วันที่ประกาศ:** 8 มิถุนายน 2555
**ปรับปรุงล่าสุด:** 8 มิถุนายน 2555
**เรื่อง:** LinkedIn ถูกแฮ็ก รหัสผ่านหลุดกว่า 6.5 ล้านชื่อ
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

LinkedIn เป็นเว็บไซต์ Social Media ที่ได้รับความนิยมในกลุ่มคนทำงาน เพราะนอกจากจะสามารถแสดงประวัติการทำงาน (Resume) ได้แล้ว ยังสามารถใช้เป็นแหล่งแลกเปลี่ยนความคิดเห็นระหว่างกลุ่มคนที่ทำงานสายอาชีพเดียวกันได้ด้วย [14-1]

เมื่อวันที่ 6 มิถุนายน 2555 เว็บไซต์ Dagens IT ของประเทศนอร์เวย์ ได้รายงานว่า มีรหัสผ่านของผู้ใช้เว็บไซต์ LinkedIn เผยแพร่อยู่บนเว็บไซต์ใต้ดินของประเทศรัสเซียกว่า 6.5 ล้านชื่อ โดยรหัสผ่านที่ถูกโพสต์นั้นเป็นรหัสผ่านที่ถูกเข้ารหัสลับไว้ (Encrypted) ซึ่งผู้ที่โพสต์นั้นมีจุดประสงค์เพื่อให้เหล่าแฮ็กเกอร์ช่วยกันแกะรหัสผ่าน ดังกล่าว (Crack) [14-2]

หน่วยงาน CERT-FI ของประเทศฟินแลนด์ แจ้งว่า ข้อมูลที่ปรากฏบนเว็บไซต์ใต้ดินนั้นมีเพียงรหัสผ่านเพียงอย่างเดียว ไม่มีชื่อผู้ใช้ แต่เชื่อว่า แฮ็กเกอร์ที่เจาะเข้าระบบได้คงจะได้ชื่อผู้ใช้ไปด้วยแล้ว [14-3]

ผู้ใช้งาน LinkedIn หลายราย ได้ตรวจสอบรหัสผ่านที่ปรากฏบนเว็บไซต์แล้วพบว่ารหัสผ่านที่เก็บอยู่ในระบบ ของ LinkedIn นั้นถูกเข้ารหัสลับด้วยฟังก์ชั่น SHA-1 โดยไม่มีการใส่ Salt ทำให้สามารถถูกแกะรหัสผ่านได้ง่ายโดยการใช้ Rainbow Table หรือใช้วิธีการ Hash Collision [14-4] [14-5]

## ผลกระทบ

รหัสผ่านบางส่วนถูกแกะได้แล้ว ดังตัวอย่างในรูปที่ 17 (14-1) ผู้ใช้ที่ตั้งรหัสผ่านตรงกับรหัสผ่านที่ถูกโพสต์ไว้ในเว็บไซต์ มีโอกาสสูงที่จะถูกขโมยหรือสวมรอยบัญชีผู้ใช้


*รูปที่ 14.รูปที่ 17 (14-1) ตัวอย่างรหัสผ่านที่ถูกแกะได้แล้ว (ที่มา Ars Technica)*

ปัจจุบัน LinkedIn มีผู้ใช้งานอยู่ประมาณ 147 ล้านคน ในจำนวนนั้นคนไทยที่ใช้งานอยู่ประมาณ 3 แสนคน [14-6] เนื่องจากข้อมูลใน LinkedIn เป็นข้อมูลส่วนบุคคลที่ใส่ไว้เพื่อผลประโยชน์ในการสมัครงานหรือทำงาน ซึ่งข้อมูลบางส่วนอาจเป็นข้อมูลสำคัญที่เป็นความลับ เช่น งานที่เคยทำ เพื่อนร่วมงาน หรือข้อมูลอื่นๆ ที่จะสามารถเห็นได้เฉพาะผู้ที่มี Connection ด้วยเท่านั้น การที่ข้อมูลบางอย่างถูกเผยแพร่ออกไป ก็อาจส่งผลต่อหน้าที่หรือการทำงานในปัจจุบันได้ นอกจากนี้ ผู้ที่ได้ข้อมูลส่วนตัวไป อาจนำข้อมูลเหล่านั้นไปปลอมตัวเป็นผู้ใช้งานเพื่อสร้างความเสียหายต่อผู้ใช้งานตัวจริงได้

## ข้อแนะนำในการป้องกันและแก้ไข

LinkedIn ได้อัพเดท Blog เพื่อชี้แจงเหตุการณ์ที่เกิดขึ้นแล้ว โดยแจ้งว่ากำลังตรวจสอบว่าเหตุการณ์นี้เกิดขึ้นได้อย่างไร และได้มีคำแนะนำสำหรับผู้ใช้ LinkedIn ที่ได้รับผลกระทบดังนี้ [14-7]

ผู้ใช้งานที่ตั้งรหัสผ่านตรงกับรหัสผ่านที่ถูกเผยแพร่ออกไป จะได้รับการแจ้งเตือนว่ารหัสผ่านดังกล่าวนั้นไม่สามารถใช้งานต่อได้ (no longer valid)

ผู้ใช้งานที่ได้รับผลกระทบจะได้รับอีเมลจาก LinkedIn เพื่อแจ้งขั้นตอนวิธีการรีเซ็ตรหัสผ่าน โดยอีเมลฉบับดังกล่าวจะไม่มีลิงก์อะไรให้ผู้ใช้คลิก มีเพียงขั้นตอนวิธีการปฏิบัติเท่านั้น หลังจากผู้ใช้ทำตามขั้นตอนดังกล่าวแล้วจะได้รับอีเมลอีกฉบับที่มีลิงก์สำหรับให้เข้าไปรีเซ็ตรหัสผ่าน

ผู้ใช้งานที่ได้รับผลกระทบ จะได้รับอีเมลจากฝ่าย Customer Support เพื่อแจ้งสถานการณ์และชี้แจงเหตุผลว่าทำไมจึงถูกขอร้องให้เปลี่ยนรหัสผ่าน

โปรแกรมเมอร์ชื่อ Fictive Kin และ Chris Shiflett ได้รวบรวม Hash ของรหัสผ่านที่ถูกเผยแพร่ และได้เปิดเว็บไซต์ http://leakedin.org/ เพื่อให้ผู้ใช้ LinkedIn ป้อนรหัสผ่านของตนเองเข้ามาตรวจสอบว่ารหัสผ่านที่ใช้ได้หลุดออกไปเผยแพร่ หรือไม่ โดยเว็บไซต์ดังกล่าวจะนำ SHA-1 ของรหัสผ่านนั้นไปตรวจสอบกับรหัสผ่านที่ถูกเผยแพร่ในเว็บไซต์ของแฮ็กเกอร์ หากผู้ใช้ท่านใดที่พบว่ารหัสผ่านของตนเองหลุดออกไปแล้ว ควรรีบเปลี่ยนรหัสผ่านโดยทันที

## อ้างอิง


[14-1] http://www.linkedin.com/static?key=what_is_linkedin&trk=hb_what

[14-2] http://translate.google.com/translate?hl=en&sl=no&tl=en&u=http://www.dagensit.no/article2411857.ece

[14-3] https://www.cert.fi/tietoturvanyt/2012/06/ttn201206061430.html

[14-4] http://thenextweb.com/socialmedia/2012/06/06/bad-day-for-linkedin-6-5-million-hashed-passwords-reportedly-leaked-change-yours-now/

[14-5] http://shiflett.org/blog/2012/jun/leakedin

[14-6] http://www.slideshare.net/amover/linkedin-demographics-statistics-jan-2012

[14-7] http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/


# 13. ระวังภัยช่องโหว่ใน MySQL/MariaDB อนุญาตให้ล็อกอินได้โดยไม่ต้องรู้รหัสผ่าน

**วันที่ประกาศ:** 11 มิถุนายน 2555
**ปรับปรุงล่าสุด:** 11 มิถุนายน 2555
**เรื่อง:** ระวังภัย ช่องโหว่ใน MySQL/MariaDB อนุญาตให้ล็อกอินได้โดยไม่ต้องรู้รหัสผ่าน
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

นักพัฒนาจาก MariaDB ได้ค้นพบช่องโหว่ในโปรแกรม MySQL และ MariaDB (MySQL เวอร์ชันที่ถูกแยกออกไปพัฒนาต่อโดยนักพัฒนาภายนอก) ซึ่งทำให้ผู้ใช้สามารถล็อกอินโดยใช้รหัสผ่านที่ไม่ถูกต้องได้ (CVE2012-2122) [15-1]

ช่องโหว่ดังกล่าวเกิดจากข้อผิดพลาดของฟังก์ชั่น memcmp() ที่ใช้ในการตรวจสอบรหัสผ่านที่รับเข้ามา ซึ่งมีบางกรณีที่ผลลัพธ์ของฟังก์ชั่นได้ค่าที่ไม่คาดคิด ทำให้โปรแกรม MySQL/MariaDB มองว่ารหัสผ่านที่รับเข้ามานั้นถูกต้อง ถึงแม้ที่จริงแล้วรหัสผ่านนั้นจะไม่ถูกต้องก็ตาม

## ผลกระทบ

หากมีผู้ใช้ที่เชื่อมต่อเข้ามาในระบบโดยป้อนชื่อผู้ใช้และรหัสผ่านอะไรก็ได้ เข้ามาซ้ำๆ กันหลายๆ ครั้ง ก็มีโอกาสที่จะผ่านเข้ามาในระบบได้ โดยส่วนใหญ่แล้ว ระบบที่ติดตั้ง MySQL/MariaDB จะใช้ชื่อผู้ใช้ว่า root เป็นค่าเริ่มต้น ซึ่งชื่อผู้ใช้ดังกล่าวมีสิทธิ์สูงสุดในระบบ ทำให้ใครก็ตามที่สามารถล็อกอินโดยใช้ชื่อผู้ใช้ดังกล่าวได้ ก็จะได้รับสิทธิ์ทั้งหมดของระบบฐานข้อมูลนั้นโดยทันที

## ระบบที่ได้รับผลกระทบ

- MySQL และ MariaDB เวอร์ชัน 5.1.61, 5.2.11, 5.3.5, 5.5.22 และต่ำกว่า
- MySQL เวอร์ชันตั้งแต่ 5.1.63, 5.5.24, 5.6.6 เป็นต้นไปไม่ได้รับผลกระทบ
- MariaDB เวอร์ชันตั้งแต่ 5.1.62, 5.2.12, 5.3.6, 5.5.23 เป็นต้นไปไม่ได้รับผลกระทบ

อย่างไรก็ตาม ข้อผิดพลาดดังกล่าวเกิดได้เฉพาะ MySQL และ MariaDB ที่คอมไพล์โดยใช้ glibc บนระบบปฏิบัติการ Linux เท่านั้น ไฟล์ไบนารีของ MySQL และ MariaDB ที่มีให้ดาวน์โหลดในเว็บไซต์ของผู้พัฒนาจะไม่มีช่องโหว่ดังกล่าวนี้

## ข้อแนะนำในการป้องกันและแก้ไข

ผู้ใช้งานโปรแกรม MySQL/MariaDB เวอร์ชันที่มีช่องโหว่ หากเป็นไปได้ ควรทำการอัพเดทโปรแกรมให้เป็นเวอร์ชันปัจจุบันโดยเร็วที่สุด

หากไม่สามารถอัพเดทได้ ผู้ใช้ควรตั้งค่าการเชื่อมต่อให้เข้ามาได้เฉพาะ localhost เพียงอย่างเดียว ด้วยการแก้ไขไฟล์ my.cnf ในส่วน [mysqld] กำหนดค่า “bind-address” ให้เป็น “127.0.0.1” จากนั้น Restart เซอร์วิสของ MySQL เพื่อให้การตั้งค่าใหม่มีผล [15-2]

## อ้างอิง


[15-1] http://seclists.org/oss-sec/2012/q2/493

[15-2] http://thehackernews.com/2012/06/cve-2012-2122-serious-mysql.html


# 14. ระวังภัยช่องโหว่ OpenType Font อาจทำเครื่องจอฟ้า

**วันที่ประกาศ:** 13 มิถุนายน 2555
**ปรับปรุงล่าสุด:** 13 มิถุนายน 2555
**เรื่อง:** ระวังภัย ช่องโหว่ OpenType Font อาจทำเครื่องจอฟ้า
**ประเภทภัยคุกคาม:** DoS (Denial of Service)

## ข้อมูลทั่วไป

นักวิจัยแจ้งเตือนช่องโหว่ 0-day ในไฟล์ ATMFD.DLL ซึ่งใช้ในการทำงานร่วมกับไฟล์ประเภท PostScript-based OpenType Font (.OTF) [16-1] ผู้ไม่หวังดีอาจโจมตีผ่านช่องโหว่นี้ผ่านไฟล์เอกสารที่สามารถฝัง (Embedded) Font ได้ เช่น

ไฟล์เอกสาร Microsoft Office หรือฝัง Font ไว้ในเว็บไซต์แล้วหลอกให้ผู้ใช้เปิดเข้าไปดู


*รูปที่ 15.รูปที่ 18 (16-1) BSoD ที่เกิดจากช่องโหว่ ATMFD.DLL [16-2]*

## ผลกระทบ

ระบบจะไม่สามารถทำงานต่อได้หาก Windows พยายามที่จะแสดงผลข้อมูลในไฟล์ Font เช่น เปิดไฟล์เอกสารหรือเข้าหน้าเว็บไซต์ที่มีการฝัง Font อันตรายดังกล่าว

- ใน Windows XP และ Server 2003 จะเกิด BSoD (Blue Screen of Death)
- ใน Windows Vista, 7 และ Server 2008 จะมีการใช้งาน CPU 100%

ตัวอย่าง BSoD ในเครื่องที่ถูกโจมตีผ่านช่องโหว่นี้ เป็นดังรูปที่ 18 (16-1)

## ระบบที่ได้รับผลกระทบ

ระบบปฏิบัติการ Windows ทั้งเวอร์ชัน 32 บิตและ 64 บิต

## ข้อแนะนำในการป้องกันและแก้ไข

ปัจจุบันช่องโหว่นี้ยังไม่มีหมายเลข CVE และยังไม่มีข้อมูลเพิ่มเติมจาก Microsoft ผู้ใช้ควรระวังในการเปิดไฟล์เอกสารที่สามารถฝัง Font ได้ เช่น ไฟล์เอกสาร Microsoft Office และควรระวังการเปิดเว็บไซต์ที่ไม่น่าเชื่อถือ

## อ้างอิง


[16-1] http://www.exploit-db.com/exploits/19089/

[16-2] http://blog.cr4.sh/2012/06/0day-windows.html


# 15. ระวังภัย ช่องโหว่ Remote Code Execution ใน Microsoft XML Core Service (CVE-2012-1889)

**วันที่ประกาศ:** 14 มิถุนายน 2555
**ปรับปรุงล่าสุด:** 14 มิถุนายน 2555
**เรื่อง:** ระวังภัย ช่องโหว่ Remote Code Execution ใน Microsoft XML Core Service (CVE-2012-1889)
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

Microsoft ประกาศ Security Advisory หมายเลข 2719615 [17-1] [17-2] แจ้งเตือนการโจมตีระบบปฏิบัติการ Windows ผ่านช่องโหว่ของ Microsoft XML Core Service ซึ่งเป็นระบบที่ใช้ในการอ่านและแสดงผลข้อมูลในไฟล์ XML [17-3] ช่องโหว่ดังกล่าวเกิดจากความผิดพลาดในการเรียกใช้ Object ที่ยังไม่ได้ Initialize ทำให้เกิดเหตุการณ์ Memory corruption ผู้ใช้อาจถูกโจมตีจากช่องโหว่นี้ผ่านเว็บไซต์ที่มีไฟล์ XML อันตรายและผ่านไฟล์เอกสาร Microsoft Office

## ผลกระทบ

ผู้ใช้ที่ใช้โปรแกรม Internet Explorer เข้าเว็บไซต์ที่มีไฟล์ XML ที่สร้างขึ้นมาเพื่อโจมตีผ่านช่องโหว่นี้ อาจถูกผู้ไม่หวังดีสั่งประมวลผลคำสั่งอันตรายจากระยะไกล (Remote Code Execution) โดยคำสั่งอันตรายดังกล่าวจะได้รับสิทธิเทียบเท่ากับสิทธิของผู้ใช้ที่กำลังล็อกอิน นอกจากนี้ ผู้ใช้ที่เปิดไฟล์เอกสาร Microsoft Office ที่มีโค้ดอันตรายแฝงอยู่ก็จะได้รับผลกระทบเช่นเดียวกัน

## ระบบที่ได้รับผลกระทบ

- Windows XP, Vista, 7, Server 2003, Server 2008 ทั้ง 32 บิตและ 64 บิต ที่ติดตั้ง Microsoft XML Core Services 3.0, 4.0, 5.0, และ 6.0
- Microsoft Office 2003 และ 2007



## ข้อแนะนำในการป้องกันและแก้ไข

Microsoft ได้ออกซอฟต์แวร์สำหรับแก้ปัญหานี้เป็นการชั่วคราวแล้ว ผู้ใช้สามารถติดตั้งได้จาก Microsoft Fix it [17-4] หากไม่สามารถติดตั้งซอฟต์แวร์ดังกล่าวได้ ควรระมัดระวังในการเปิดเว็บไซต์ด้วยโปรแกรม Internet Explorer หรือระมัดระวังการเปิดไฟล์เอกสาร Microsoft Office ที่น่าสงสัย

โดยปกติแล้วโปรแกรม Internet Explorer บน Windows Server 2003, 2008 และ 2008 R2 จะทำงานในโหมด Enhanced Security Configuration [17-5] ซึ่งสามารถลดผลกระทบที่เกิดจากช่องโหว่นี้ได้ อย่างไรก็ตาม Microsoft ได้แนะนำให้ผู้ใช้ตั้งค่า EMET [17-6] ให้กับโปรแกรม Internet Explorer เพิ่มเติมด้วย

## อ้างอิง


[17-1] https://technet.microsoft.com/en-us/security/advisory/2719615

[17-2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1889

[17-3] http://msdn.microsoft.com/en-us/data/bb291077.aspx

[17-4] http://support.microsoft.com/kb/2719615

[17-5] http://technet.microsoft.com/en-us/library/dd883248(WS.10).aspx

[17-6] http://www.thaicert.or.th/papers/technical/2012/pp2012te0004.html


# 16. ระวังภัย ช่องโหว่ Remote Code Execution ใน Internet Explorer (CVE2012-1875)

**วันที่ประกาศ:** 19 มิถุนายน 2555
**ปรับปรุงล่าสุด:** 19 มิถุนายน 2555
**เรื่อง:** ระวังภัย ช่องโหว่ Remote Code Execution ใน Internet Explorer (CVE2012-1875)
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

Microsoft ประกาศ Security Bulletin รหัส MS12-037 [18-1] เพื่อแจ้งเตือนการโจมตีผ่านช่องโหว่ Same ID Property Remote Code Execution ใน Internet Explorer (CVE2012-1875) [18-2] ช่องโหว่ดังกล่าวเกิดขึ้นเมื่อหน้าเว็บไซต์นั้นมี Object ที่ถูกประกาศชื่อ ID ซ้ำกัน แล้วมีการลบ Object ตัวใดตัวหนึ่งออก (เช่น ถูกลบโดย JavaScript) เมื่อมีการเรียกใช้ Object ที่มีชื่อ ID ดังกล่าว Internet Explorer จะไปอ่านข้อมูลจากหน่วยความจำในตำแหน่งที่ไม่ได้ใช้งานแล้ว (Use after free) ทำให้โปรแกรมทำงานผิดพลาด ปัจจุบันมีโค้ดเพื่อใช้โจมตีผ่านช่องโหว่ดังกล่าวเผยแพร่ในอินเทอร์เน็ตแล้ว [18-3] [18-4] [18-5]

## ผลกระทบ

ผู้โจมตีสามารถสร้างเว็บไซต์อันตรายแล้วหลอกให้เหยื่อเข้าไป เมื่อเหยื่อเปิดเว็บไซต์โดยใช้โปรแกรม Internet Explorer อาจถูกผู้ไม่หวังดีสั่งประมวลผลคำสั่งอันตรายจากระยะไกลได้ (Remote Code Execution) โดยผู้โจมตีจะได้รับสิทธิในการทำงานเท่ากับสิทธิของผู้ใช้ที่ล็อกอิน

## ระบบที่ได้รับผลกระทบ

Internet Explorer เวอร์ชัน 6, 7, 8 และ 9 บนระบบปฏิบัติการ Windows ทั้ง 32 บิตและ 64 บิต

## ข้อแนะนำในการป้องกันและแก้ไข

Microsoft ได้ออกแพทช์หมายเลข 2699988 เพื่อแก้ไขปัญหาดังกล่าวแล้ว ผู้ใช้สามารถดาวน์โหลดได้จาก http://support.microsoft.com/kb/2699988

## อ้างอิง


[18-1] http://technet.microsoft.com/en-us/security/bulletin/ms12-037

[18-2] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1875

[18-3] http://pastebin.com/sFqxs4qx

[18-4] http://www.youtube.com/watch?v=b2_SEx6aBCI

[18-9] http://nakedsecurity.sophos.com/2012/06/19/ie-remote-code-execution-vulnerability-being-actively-exploited-in-the-wild/


# 17. ระวังภัย ช่องโหว่ Remote Code Execution ใน Windows Sidebar/Gadget

**วันที่ประกาศ:** 12 กรกฎาคม 2555
**ปรับปรุงล่าสุด:** 12 กรกฎาคม 2555
**เรื่อง:** ระวังภัย ช่องโหว่ Remote Code Execution ใน Windows Sidebar/Gadgets
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

Windows Sidebar เป็นคุณสมบัติที่มีใน Windows Vista โดยจะปรากฏเป็นแถบยาวแนวตั้งอยู่ทางขวาของ Desktop ภายในสามารถบรรจุ Gadgets ซึ่งเป็นโปรแกรมย่อยที่ช่วยอำนวยความสะดวกในการทำงานหรือติดตามข้อมูล เช่น แสดงนาฬิกา แสดงเปอร์เซนต์การใช้ CPU แสดง RSS Feed เป็นต้น [19-1] ใน Windows Vista นั้น Gadgets จะถูกจำกัดไว้ใน Sidebar แต่ใน Windows 7 ทาง Microsoft ได้ตัด Windows Sidebar ออกไป และปรับปรุงให้ Gadgets สามารถอยู่บนหน้า Desktop ได้อย่างอิสระ พร้อมทั้งเรียกชื่อคุณสมบัติใหม่นี้ว่า Windows Gadgets [19-2] ตัวอย่าง Windows Sidebar เป็นดังรูปที่ 19 (19-1) และตัวอย่าง Windows Gadgets เป็นดังรูปที่ 20 (19-2)

รูปที่ 20 (19-2) Windows Gadgets ใน Windows 7 [19-2]

เมื่อวันที่ 10 กรกฎาคม 2555 Microsoft ประกาศ Security Advisory รหัส KB2719662 เพื่อแจ้งเตือนการโจมตีผ่านช่องโหว่ใน Windows Sidebar และ Windows Gadgets พร้อมปล่อยซอฟต์แวร์ Fix it เพื่อแก้ไขปัญหาดังกล่าว [19-3]


*รูปที่ 16.รูปที่ 19 (19-1) Windows Sidebar ใน Windows Vista [19-1]*

*รูปที่ 17.รูปที่ 20 (19-2) Windows Gadgets ใน Windows 7 [19-2]*

## ผลกระทบ

ผู้ไม่ประสงค์ดีสามารถสร้างไฟล์ Gadgets (.gadget) ที่มีคำสั่งโจมตีผ่านช่องโหว่ดังกล่าวอยู่ หากผู้ใช้ติดตั้ง Gadgets นั้นลงในระบบโดยไม่ตั้งใจ อาจถูกผู้ไม่ประสงค์ดีสั่งประมวลผลคำสั่งอันตรายจากระยะไกลได้ (Remote Code Execution) โดยผู้ไม่ประสงค์ดีจะได้รับสิทธิในการทำงานเท่ากับสิทธิของผู้ใช้ที่ล็อกอิน

## ระบบที่ได้รับผลกระทบ

Windows Vista และ Windows 7 ทั้งเวอร์ชัน 32 บิตและ 64 บิต

## ข้อแนะนำในการป้องกันและแก้ไข

Microsoft ได้ออกซอฟต์แวร์ Fix it 50907 เพื่อปิดการทำงานของ Windows Sidebar/Gadgets โดยซอฟต์แวร์ดังกล่าวนี้เป็นการปิดการทำงานเพื่อแก้ปัญหาแบบชั่วคราวระหว่าง รอแพทช์แก้ไขช่องโหว่ต่อไป ผู้ใช้สามารถดาวน์โหลดซอฟต์แวร์ Fix it ได้จาก เว็บไซต์ของ Microsoft [19-4]

ปัจจุบัน Microsoft ได้ยกเลิกบริการดาวน์โหลด Gadgets จากหน้าเว็บไซต์ของ Microsoft แล้ว [19-5] แต่ผู้ใช้ยังสามารถดาวน์โหลดและติดตั้ง Gadgets จากเว็บไซต์อื่นๆ ได้ตามปกติ อย่างไรก็ตาม การติดตั้ง Gadgets จากแหล่งที่มาที่ไม่น่าเชื่อถืออาจเป็นอันตรายต่อระบบได้ ผู้ใช้ควรพิจารณาให้รอบคอบก่อนทำการติดตั้ง Gadget ใดๆ ลงในเครื่อง โดยอาจติดตั้งเฉพาะ Gadgets จากบริษัทที่มีความน่าเชื่อถือ และหลีกเลี่ยงการติดตั้ง Gadgets จากนักพัฒนาภายนอก

## อ้างอิง


[19-1] http://windows.microsoft.com/en-US/windows-vista/Windows-Sidebar-and-gadgets-overview

[19-2] http://windows.microsoft.com/en-us/windows7/products/features/gadgets

[19-3] http://technet.microsoft.com/en-us/security/advisory/2719662

[19-4] http://support.microsoft.com/kb/2719662

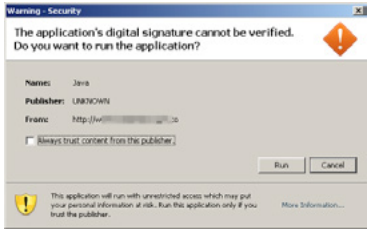
[19-5] http://windows.microsoft.com/th-TH/windows/downloads/personalize/gadgets

# 18. ระวังภัยโทรจัน GetShell.A ทำงานได้ทั้งบน Windows, Mac และ Linux

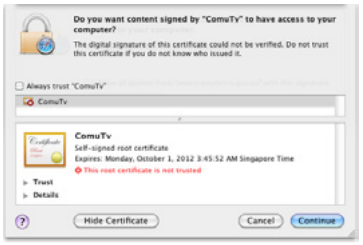
**วันที่ประกาศ:** 12 กรกฎาคม 2555
**ปรับปรุงล่าสุด:** 12 กรกฎาคม 2555
**เรื่อง:** ระวังภัย โทรจัน GetShell.A ทำงานได้ทั้งบน Windows, Mac และ Linux
**ประเภทภัยคุกคาม:** Malicious Code

## ข้อมูลทั่วไป

บริษัท F-Secure ผู้พัฒนาโปรแกรมแอนตี้ไวรัส ได้ค้นพบวิธีการเผยแพร่โปรแกรมไม่พึงประสงค์บนหน้าเว็บไซต์ที่ถูกแฮ็ก [20-1] [20-2] ผู้ไม่ประสงค์ดีฝัง Java applet ไว้ในเว็บไซต์ เมื่อผู้ใช้เข้ามายังเว็บไซต์ดังกล่าวก็จะพบกับหน้าต่างขอยืนยันการทำงานของ Java applet ที่ถูก Sign โดย CA ที่ไม่น่าเชื่อถือ (Untrusted) ดังรูปที่ 21 (20-1) และ 22 (20-2)




*รูปที่ 18.รูปที่ 21 (20-1) หน้าต่างขอยืนยันการทำงานของ Java applet ไม่พึงประสงค์บนระบบปฏิบัติการ Windows*




*รูปที่ 19.รูปที่ 22 (20-2) หน้าต่างขอยืนยันการทำงานของ Java applet ไม่พึงประสงค์บนระบบปฏิบัติการ Mac OS X*

## ผลกระทบ

หากผู้ใช้อนุญาตให้ Java applet ดังกล่าวทำงาน applet นั้นจะตรวจสอบเครื่องของผู้ใช้ว่าเป็นระบบปฏิบัติการอะไร จากนั้นจะเชื่อมต่อไปยังเครื่อง C&C เพื่อดาวน์โหลดโทรจัน GetShell.A มาติดตั้งลงในเครื่องของผู้ใช้

โทรจัน GetShell.A เป็น Backdoor ที่จะเปิดพอร์ตไว้เพื่อรอให้ผู้ไม่ประสงค์ดีเชื่อมต่อเข้ามาสั่งงานเครื่อง คอมพิวเตอร์ที่ตกเป็นเหยื่อให้ประมวลผลคำสั่งไม่พึงประสงค์ [20-3]

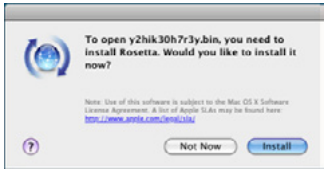
## ระบบที่ได้รับผลกระทบ

จากข้อมูลในไฟล์ Java applet ดังรูปที่ 23 (20-3) แสดงให้เห็นว่า โปรแกรมไม่พึงประสงค์ดังกล่าวสามารถทำงานได้ทั้งบนระบบปฏิบัติการ Windows เวอร์ชัน 32 บิตและ 64 บิต รวมทั้งระบบปฏิบัติการ Mac OS X และ Linux ด้วย

*รูปที่ 20.รูปที่ 23 (20-3) ข้อมูลในไฟล์ Java applet*



อย่างไรก็ตาม โทรจัน GetShell.A บนระบบปฏิบัติการ Mac OS X นั้นจะทำงานได้บนเครื่องที่ใช้ CPU PowerPC เท่านั้น หากนำไฟล์นี้มารันบนเครื่องที่เป็น CPU Intel ระบบจะแสดงหน้าจอแจ้งเตือนว่าต้องรันผ่านโปรแกรม Rosetta ดังรูปที่ 24 (20-4)




*รูปที่ 21.รูปที่ 24 (20-4) หน้าจอการแจ้งเตือนว่าต้องรันโทรจันผ่านโปรแกรม Rosetta*

## ข้อแนะนำในการป้องกันและแก้ไข

หากผู้ใช้ตกเป็นเหยื่อของโทรจัน GetShell.A สามารถกำจัดโทรจันนี้ออกจากระบบได้โดยใช้โปรแกรมแอนตี้ไวรัสที่ได้รับการอัพเดทฐานข้อมูลเป็นเวอร์ชันล่าสุด

อย่างไรก็ตาม เพื่อเป็นการป้องกันความเสียหายที่อาจจะเกิดขึ้นได้ในอนาคต ผู้ใช้ไม่ควรเข้าชมเว็บไซต์ที่ไม่รู้จัก เช่น ไม่ควรคลิกลิงก์ที่มากับอีเมล เป็นต้น รวมทั้งก่อนการคลิกอนุญาตให้รัน Java applet บนเว็บไซต์ใดๆ ผู้ใช้ควรตรวจสอบให้แน่ใจว่าต้องการรัน applet นั้นจริงๆ หากไม่แน่ใจควรปิดเว็บไซต์นั้นทันที เพราะ applet ดังกล่าวอาจนำมาซึ่งโปรแกรมไม่พึงประสงค์ก็ได้

## อ้างอิง

[20-1] https://www.f-secure.com/weblog/archives/00002397.html

[20-2] http://www.computerworld.com/s/article/9228972/Java_based_Web_attack_installs_backdoors_on_Windows_Linux_Mac_computers

[20-3] http://www.microsoft.com/security/portalhrEnEntaspx?Name=TrojanDownloader%3AJava%2FGetShell.A&ThreatID=-2147308694

# 19. Yahoo! Contributor Network ถูกเจาะ บัญชีผู้ใช้ 453,492 รายหลุดเป็น plaintext

**วันที่ประกาศ:** 12 กรกฎาคม 2555
**ปรับปรุงล่าสุด:** 13 กรกฎาคม 2555
**เรื่อง:** Yahoo! Contributor Network ถูกเจาะ บัญชีผู้ใช้ 453,492 รายหลุดเป็น plaintext
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

แฮ็กเกอร์โพสต์ข้อมูลบัญชีผู้ใช้บริการบางอย่างของ Yahoo! จำนวน 453,492 รายลงในเว็บไซต์แห่งหนึ่ง โดยอ้างว่าได้ข้อมูลดังกล่าวมาด้วยวิธีการทำ SQL Injection แบบ Union ซึ่งข้อมูลบัญชีผู้ใช้ทั้งหมดที่ถูกโพสต์นั้นเป็น plaintext ไม่มีการเข้ารหัสลับแต่อย่างใด [21-1] [21-2] ตัวอย่างข้อมูลที่ถูกโพสต์เป็นดังรูปที่ 25 (21-1)

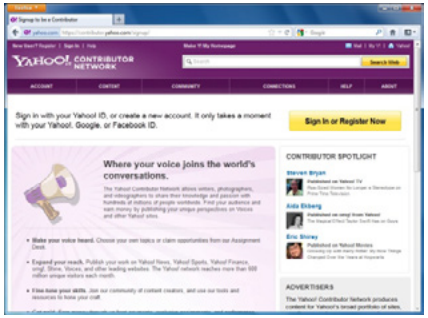
```
64203:ea          @yahoo.co.th:ea
64204:ch          @msn.com:am
64205:to          @yahoo.com:wi
```

*รูปที่ 22.รูปที่ 25 (21-1) ตัวอย่างข้อมูลบัญชีผู้ใช้บริการของ Yahoo! ที่ถูกโพสต์*

ผู้ที่โพสต์ข้อมูลบัญชีผู้ใช้ไม่ได้ระบุว่าบริการของ Yahoo! นั้นคือบริการอะไร แต่จากการวิเคราะห์ของเว็บไซต์ TrustedSec คาดว่าเป็นบริการ Yahoo! Voices เนื่องจากตรวจสอบพบข้อความ dbb1.ac.bf1.yahoo.com อยู่ในไฟล์ที่ถูกเผยแพร่ ซึ่งเป็นเซิร์ฟเวอร์ของบริการ Yahoo! Voices [21-3]

ล่าสุดทาง Yahoo! ได้ออกแถลงการณ์ในเรื่องดังกล่าว โดยชี้แจงว่าข้อมูลที่หลุดออกมานั้นเป็นข้อมูลเก่าของ Yahoo! Contributor Network (http://contributor.yahoo.com) ซึ่งเป็นบริการรวมรวมข้อมูลข่าวสารที่ผู้ใช้สร้าง เช่น บทความ ภาพถ่าย คลิปวิดีโอ เพื่อนำขึ้นไปเผยแพร่ในบริการต่างๆ ของ Yahoo! (เช่น Yahoo! Voices หรือ Yahoo! News) ดังแสดงในรูปที่

26 (21-2) ซึ่งบริการดังกล่าวนี้อนุญาตให้ผู้ใช้สามารถใช้อีเมลอื่นในการสมัครได้ โดยไม่จำเป็นที่จะต้องใช้ Yahoo! Mail เพียงอย่างเดียว [21-4]




*รูปที่ 23.รูปที่ 26 (21-2) หน้าเว็บไซต์ของ Yahoo! Contributor Network*

นอกจากนี้ ทาง Yahoo! ได้ชี้แจงเพิ่มเติมว่า รหัสผ่านในบัญชีผู้ใช้ตามรายชื่อที่ถูกเผยแพร่ออกไปนั้นมีจำนวนไม่ถึง 5% ที่ยังสามารถใช้งานได้ อย่างไรก็ตาม ทาง Yahoo! แจ้งว่ากำลังปรับปรุงแก้ไขช่องโหว่ที่พบ และได้เปลี่ยนรหัสผ่านให้กับผู้ใช้ที่ได้รับผลกระทบจากเหตุการณ์ดังกล่าวแล้ว

## ผลกระทบ

ผู้ที่ใช้บริการของ Yahoo! ที่มีรายชื่ออยู่ในข้อมูลที่ถูกเผยแพร่อาจถูกสวมรอยบัญชีผู้ใช้ได้

## ระบบที่ได้รับผลกระทบ

ผู้ใช้บริการ Yahoo! Contributor Network มีความเสี่ยงที่จะได้รับผลกระทบโดยตรง แต่เนื่องจากบริการดังกล่าวนี้มีความเชื่อมโยงกับบริการอื่นๆ ของ Yahoo! ด้วย ดังนั้นผู้ที่ใช้งานบริการต่างๆ ของ Yahoo! ตามรายชื่อต่อไปนี้ อาจได้รับผลกระทบตามไปด้วย

- Yahoo! Voices (http://voices.yahoo.com/)
- Yahoo! News (http://news.yahoo.com/)
- Yahoo! Local (http://local.yahoo.com/)
- Yahoo! Local (http://sports.yahoo.com/)
- Yahoo! Sports (http://finance.yahoo.com/)
- Yahoo! Finance (http://finance.yahoo.com/)
- Yahoo! TV (http://tv.yahoo.com/)
- Yahoo! Movies (http://movies.yahoo.com/)
- Yahoo! Shopping (http://shopping.yahoo.com/)
- omg! shine (http://omg.yahoo.com/)

## ข้อแนะนำในการป้องกันและแก้ไข

บริษัท Sucuri ซึ่งเป็นบริษัทที่ทำวิจัยเกี่ยวกับ Malware ได้พัฒนาเว็บไซต์เพื่อช่วยเหลือผู้ใช้บริการของ Yahoo! ในการตรวจสอบอีเมลของตนเองว่าอยู่ในรายชื่อที่ถูกเผยแพร่หรือไม่ โดยสามารถตรวจสอบได้ที่เว็บไซต์ http://labs.sucuri.net/?yahooleak

อย่างไรก็ตาม เพื่อเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้น ผู้ใช้บริการของ Yahoo! ควรรีบเปลี่ยนรหัสผ่านที่ใช้งานโดยทันที

## อ้างอิง


[21-1] http://arstechnica.com/security/2012/07/yahoo-service-hacked/

[21-2] http://thenextweb.com/insider/2012/07/12/yahoo-gets-hacked-as-400000-plaintext-credentials-are-posted-online/

[21-3] https://www.trustedsec.com/july-2012/yahoo-voice-website-breached-400000-compromised/

[21-4] http://techcrunch.com/2012/07/12/yahoo-confirms-apologizes-for-the-email-hack-says-still-fixing-plus-check-if-you-were-impacted-non-yahoo-accounts-apply/



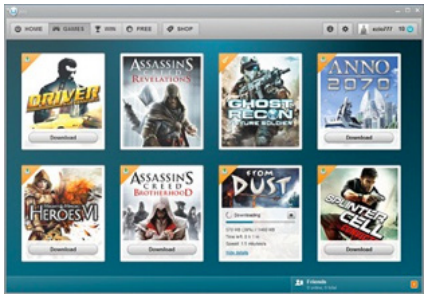

# 20. ระวังภัยช่องโหว่ในซอฟต์แวร์ Uplay ของ Ubisoft แฮ็กเกอร์สามารถสั่งเปิดโปรแกรมในเครื่องเหยื่อได้

**วันที่ประกาศ:** 31 กรกฎาคม 2555
**ปรับปรุงล่าสุด:** 31 กรกฎาคม 2555
**เรื่อง:** ระวังภัย ช่องโหว่ในซอฟต์แวร์ Uplay ของ Ubisoft แฮ็กเกอร์สามารถสั่งเปิดโปรแกรมในเครื่องเหยื่อได้
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

DRM ย่อมาจาก Digital Right Management เป็นระบบป้องกันการละเมิดลิขสิทธิ์ ซึ่งนิยมใช้ในการควบคุมการใช้งานหรือการเผยแพร่ข้อมูลดิจิทัล เช่น ซอฟต์แวร์ เพลง หรือภาพยนตร์ เป็นต้น [22-1]

Uplay เป็นซอฟต์แวร์ DRM ของบริษัท Ubisoft ซึ่งใช้ในการ Activate เกมที่ผู้ใช้ซื้อมาผ่านทางเว็บไซต์ Uplay ระบบดังกล่าวถูกนำมาใช้ครั้งแรกในเกม Assassin's Creed 2 ซึ่งวางจำหน่ายเมื่อปี พ.ศ. 2552 เมื่อผู้ใช้ติดตั้งเกมของ Ubisoft โปรแกรม Uplay จะถูกติดตั้งมาเป็นปลั๊กอินของเบราว์เซอร์ด้วย [22-2] ตัวอย่างโปรแกรม Uplay เป็นดังรูปที่ 27 (22-1)




*รูปที่ 24.รูปที่ 27 (22-1) โปรแกรม Uplay (ที่มา http://uplay.ubi.com)*

นาย Tavis Ormandy ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจาก Google ได้รายงานการค้นพบช่องโหว่ของโปรแกรม Uplay ที่ถูกติดตั้งมาพร้อมกับเกม Assassin's Creed Revelation ใน Full Disclosure Mailing List พร้อมเผยแพร่ตัวอย่างโค้ดที่ใช้ทดสอบการทำงานของช่องโหว่ดังกล่าว [22-3]

## ผลกระทบ

โปรแกรม Uplay สามารถเรียกใช้งานโปรแกรมใดๆ ในเครื่องได้ผ่านทางเว็บเบราว์เซอร์ ผู้ไม่หวังดีสามารถสร้างหน้าเว็บไซต์ที่มีโค้ด JavaScript เพื่อสั่งรันไฟล์ใดๆ ก็ได้ในเครื่องของเหยื่อ [22-4]

## ระบบที่ได้รับผลกระทบ

เครื่องที่ใช้งานระบบปฏิบัติการ Windows ที่ติดตั้งเกมของ Ubisoft ที่ใช้งานระบบ Uplay ดังนี้ [22-5]

- Anno 2070
- Assassin's Creed II
- Assassin's Creed: Brotherhood
- Assassin's Creed: Project Legacy
- Assassin's Creed Revelations
- Assassin's Creed III
- Beowulf: The Game
- Brothers in Arms: Furious 4
- Call of Juarez: The Cartel
- Driver: San Francisco
- Heroes of Might and Magic VI
- Just Dance 3
- Prince of Persia: The Forgotten Sands
- Pure Football
- R.U.S.E.
- Shaun White Skateboarding
- Silent Hunter 5: Battle of the Atlantic
- The Settlers 7: Paths to a Kingdom
- Tom Clancy's H.A.W.X. 2
- Tom Clancy's Ghost Recon: Future Soldier
- Tom Clancy's Splinter Cell: Conviction
- Your Shape: Fitness Evolved

## ข้อแนะนำในการป้องกันและแก้ไข

บริษัท Ubisoft ได้เผยแพร่โปรแกรม Uplay เวอร์ชัน 2.04 ที่ได้แก้ไขช่องโหว่นี้แล้ว โดยจะอนุญาตให้ปลั๊กอิน Uplay ในเว็บเบราว์เซอร์เรียกใช้งานได้แค่โปรแกรมของ Uplay เท่านั้น [22-6] ซึ่งสามารถดาวน์โหลดได้จากเว็บไซต์ http://uplay.ubi.com ผู้ใช้สามารถตรวจสอบเวอร์ชันของโปรแกรม Uplay ที่ถูกติดตั้งในเครื่องได้โดยการคลิกปุ่มรูปตัว i ที่มุมขวาบนของหน้าต่างโปรแกรม

โปรแกรม Mozilla Firefox ได้จัดให้ปลั๊กอิน Uplay อยู่ใน Blocker List แล้ว เพื่อป้องกันการโจมตีจากช่องโหว่ดังกล่าว [22-7]

สำหรับผู้ที่ต้องการตรวจสอบว่าเครื่องคอมพิวเตอร์ที่ใช้งานอยู่นั้นปลอดภัยหรือไม่ สามารถตรวจสอบได้จากเว็บไซต์ Proof-of-concept code ที่ http://pastehtml.com/view/c6gxl1a79.html หากปรากฏหน้าต่างโปรแกรม Calculator แสดงว่าระบบมีช่องโหว่ ควรอัพเดทโปรแกรม Uplay โดยทันที

## อ้างอิง


[22-1] http://computer.howstuffworks.com/drm1.htm

[22-2] http://www.kotaku.com.au/2009/11/ubisoft-all-our-games-will-do-this-uplay-thing/

[22-3] http://seclists.org/fulldisclosure/2012/Jul/375

[22-4] http://www.h-online.com/security/news/item/Ubisoft-DRM-opens-backdoor-1655653.html

[22-5] http://en.wikipedia.org/wiki/Ubisoft#Uplay

[22-6] http://forums.ubi.com/showthread.php/699756-Ubisoft-DRM-rootkit-may-allow-access-to-PC-files?s=14dfb48e3f481a0a8c6aabc8da7fbc0b&p=8510888&viewfull=1#post8510888

[22-7] https://addons-dev.allizom.org/en-US/firefox/blocked/p103


# 21. นักวิจัยสาธิตมัลแวร์ที่ติดในเฟิร์มแวร์ EFI ของเครื่อง Mac

**วันที่ประกาศ:** 1 สิงหาคม 2555
**ปรับปรุงล่าสุด:** 1 สิงหาคม 2555
**เรื่อง:** นักวิจัยสาธิตมัลแวร์ที่ติดในเฟิร์มแวร์ EFI ของเครื่อง Mac
**ประเภทภัยคุกคาม:** Malicious Code, Intrusion

## ข้อมูลทั่วไป

EFI หรือ Extensible Firmware Interface เป็นเฟิร์มแวร์ที่ถูกออกแบบมาเพื่อใช้แทน BIOS เนื่องจากเทคโนโลยีใน BIOS นั้นมีข้อจำกัดและไม่สามารถรองรับกับอุปกรณ์ใหม่ๆ ที่ออกมาได้ เช่น ไม่สามารถบู๊ตจากฮาร์ดดิสก์ที่มีขนาดใหญ่กว่า 2 TB ได้ เป็นต้น

EFI ถูกคิดค้นและพัฒนาขึ้นโดยบริษัท Intel ในปี พ.ศ. 2541 และได้ออกมาตรฐาน EFI เวอร์ชัน 1.10 ในปี พ.ศ. 2548 จากนั้นได้เปลี่ยนให้องค์กร Unified EFI Consortium เป็นผู้ดูแล จึงได้เปลี่ยนชื่อใหม่เป็น Unified Extensible Firmware Interface (UEFI) [23-1] ในปี พ.ศ. 2549 บริษัท Apple Inc. ได้ผลิตเครื่องคอมพิวเตอร์ Macintosh ที่ใช้ CPU ของ Intel และได้เริ่มใช้เทคโนโลยี EFI ในคอมพิวเตอร์ตระกูล Macintosh ตั้งแต่นั้นเป็นต้นมา โดยเทคโนโลยี EFI ที่ Apple นำมาใช้นั้นอ้างอิงตามมาตรฐาน EFI เวอร์ชัน 1.10 [23-2]

ในงาน Black Hat USA 2012 นักวิจัยด้านความมั่นคงปลอดภัยได้สาธิตมัลแวร์ประเภท Rootkit ที่สามารถแทรกตัวเองลงในเฟิร์มแวร์ EFI ของเครื่อง Mac Book Air และสามารถข้ามการทำงาน (Bypass) ของระบบ FileVault ซึ่งเป็นระบบเข้ารหัสลับข้อมูลในฮาร์ดดิสก์ได้

## ผลกระทบ

มัลแวร์ที่นักวิจัยนำมาสาธิตนี้สามารถแก้ไข Kernel ของระบบปฏิบัติการ รวมถึงทำงานเป็น Keylogger เพื่อดักรหัสผ่านที่ใช้ในการถอดรหัสลับดิสก์ที่ถูกเข้ารหัสลับด้วยระบบ FileVault ได้ นอกจากนี้นักวิจัยยังได้ให้ข้อมูลเพิ่มเติมว่ามัลแวร์ดังกล่าวนี้สามารถดัดแปลงให้มีความสามารถอื่นๆ เพิ่มเติมได้ด้วย เช่น เปิด Reverse Shell เพื่อให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องจากระยะไกลได้ เป็นต้น [23-3]

การแพร่กระจายของมัลแวร์ดังกล่าวนี้ อาจทำได้ด้วยการเสียบ USB Drive ที่มีโค้ดของมัลแวร์เข้าไปในเครื่องของเหยื่อ หรือเสียบอุปกรณ์ Thunderbolt-to-Ethernet ที่ถูกดัดแปลงโดยใส่ไดรเวอร์พิเศษเข้าไป จากนั้นเมื่อเปิดเครื่องคอมพิวเตอร์เครื่องของเหยื่อก็จะนำโค้ดอันตรายดังกล่าวไปประมวลผลโดยอัตโนมัติ

## ระบบที่ได้รับผลกระทบ

เครื่องคอมพิวเตอร์ตระกูล Macintosh ที่ใช้ระบบ EFI (เครื่องที่วางจำหน่ายตั้งแต่ปี พ.ศ. 2549 เป็นต้นไป)

## ข้อแนะนำในการป้องกันและแก้ไข

มัลแวร์ที่นักวิจัยนำมาสาธิตนี้ถูกสร้างขึ้นมาเพื่อแสดงให้เห็นถึงช่องโหว่ และไม่ได้นำไปแพร่กระจายในสาธารณะ แต่อย่างไรก็ตาม อาจมีผู้ไม่หวังดีนำช่องโหว่ดังกล่าวนี้ไปสร้างมัลแวร์เพื่อโจมตีผู้ใช้งานทั่วไปได้

การป้องกันตัวจากการโจมตีผ่านช่องโหว่ดังกล่าว อาจทำได้หลายวิธี เช่น การตั้งรหัสผ่านในขั้นตอน BDS (Boot Device Selection) ซึ่งเป็นขั้นตอนที่ให้ผู้ใช้เลือกว่าจะบู๊ตจากอุปกรณ์อะไร ซึ่งวิธีการดังกล่าวสามารถป้องกันการโจมตีจากอุปกรณ์เชื่อมต่อภายนอก เช่น USB Drive, Firewire หรือ Network Interface ได้เท่านั้น แต่ไม่สามารถป้องกันการโจมตีโดยการเสียบอุปกรณ์เข้ากับ PCI Bus ของเครื่องโดยตรงได้ เช่น ExpressCard หรือ Thunderbolt [23-4]

เนื่องจากมัลแวร์ดังกล่าวนี้จะทำงานได้ก็ต่อเมื่อผู้โจมตีสามารถเชื่อมต่ออุปกรณ์ เช่น USB Drive เข้ากับเครื่องคอมพิวเตอร์ของเหยื่อ ดังนั้นหากผู้ใช้ตรวจสอบพอร์ตของเครื่องก่อนทำการเปิดเครื่อง ก็อาจช่วยป้องกันการโจมตีจากผู้ไม่หวังดีได้

## อ้างอิง


[23-1] http://h30565.www3.hp.com/t5/Feature-Articles/The-30-year-long-Reign-of-BIOS-is-Over-Why-UEFI-Will-Rock-Your/ba-p/198

[23-2] http://www.everymac.com/mac-answers/macintel-faq/intel-macs-openfirmware-bios-altivec-firewire-powerpc.html#bios

[23-3] http://www.h-online.com/security/news/item/EFI-rootkit-for-Macs-demonstrated-1655108.html

[23-4] http://ho.ax/De_Mysteriis_Dom_Jobsivs_Black_Hat_Paper.pdf

# 22. ระวังภัย ช่องโหว่ CVE-2012-4681 ใน Java 7

**วันที่ประกาศ:** 28 สิงหาคม 2555
**ปรับปรุงล่าสุด:** 24 ตุลาคม 2555
**เรื่อง:** ระวังภัย ช่องโหว่ CVE-2012-4681 ใน Java 7
**ประเภทภัยคุกคาม:** Malicious Code, Intrusion

## ข้อมูลทั่วไป

บริษัท FireEye ซึ่งเป็นบริษัทที่วิเคราะห์และพัฒนาเครื่องมือที่เกี่ยวข้องกับระบบ Security ได้ค้นพบการโจมตีผ่านช่องโหว่ของโปรแกรม Java Runtime เวอร์ชัน 7 Update 6 (build 1.7.0_06) โดยโจมตีผ่านการฝัง Java Applet ไว้ในเว็บไซต์ [24-1] ช่องโหว่ดังกล่าวนี้ถูกกำหนดหมายเลขเป็น CVE-2012-4681 [24-2]

## ผลกระทบ

เมื่อผู้ใช้เข้าไปยังเว็บไซต์ที่มี Java Applet อันตรายอยู่ จะถูก Applet ดังกล่าวนี้ดาวน์โหลดโปรแกรมไม่พึงประสงค์มาติดตั้งลงในเครื่อง ดังรูปที่ 28 (24-1) ซึ่งโปรแกรมดังกล่าวนี้เปิดโอกาสให้ผู้ไม่หวังดีสั่งประมวลผลคำสั่งอันตรายจากระยะไกลได้ (Remote Code Execution) [24-3]

*รูปที่ 25.รูปที่ 28 (24-1) โปรแกรมไม่พึงประสงค์ที่ถูกดาวน์โหลดมาติดตั้ง (ที่มา FireEye)*

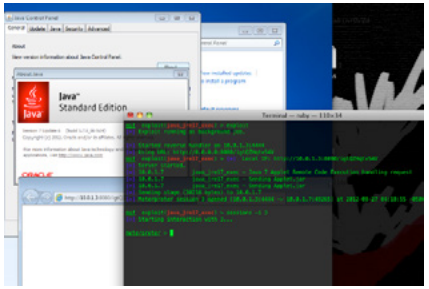
## ระบบที่ได้รับผลกระทบ

ทีมพัฒนา Metasploit ซึ่งเป็นซอฟต์แวร์ที่ใช้สำหรับทดสอบช่องโหว่ของระบบ (Penetration Testing) ได้ทดลองสร้างชุดคำสั่งที่โจมตีผ่านช่องโหว่ดังกล่าว และพบว่าคำสั่งนี้สามารถทำงานได้บนระบบที่ติดตั้ง Java Runtime เวอร์ชัน 7 ตั้งแต่ Update 0 จนถึง Update 6 ผ่านทางเบราว์เซอร์บนระบบปฏิบัติการดังต่อไปนี้ [24-4]

- Mozilla Firefox บน Ubuntu 10.04
- Internet Explorer, Mozilla Firefox และ Google Chrome บน Windows XP
- Internet Explorer และ Mozilla Firefox บน Windows Vista
- Internet Explorer และ Mozilla Firefox บน Windows 7
- Safari บน OS X 10.7.4

อย่างไรก็ตาม ช่องโหว่ดังกล่าวนี้อาจทำงานได้บนระบบปฏิบัติการใดๆ ที่ใช้เบราว์เซอร์อื่นๆ ได้อีก หากมีความคืบหน้าเพิ่มเติมทางไทยเซิร์ตจะแจ้งให้ทราบต่อไป

ตัวอย่าง การโจมตีโดยใช้ซอฟต์แวร์ Metasploit เป็นดังรูปที่ 29 (24-2)




*รูปที่ 26.รูปที่ 29 (24-2) ตัวอย่างการใช้ Metasploit โจมตี Windows 7 ผ่านช่องโหว่ CVE-2012-4681 (ที่มา Rapid7)*

## ข้อแนะนำในการป้องกันและแก้ไข

ในวันที่ 31 สิงหาคม 2555 บริษัท Oracle ผู้ผลิตซอฟต์แวร์ Java Runtime ได้ปล่อยโปรแกรม Java 7 Update 7 (build 1.7.0_07) ซึ่งแก้ไขช่องโหว่นี้แล้ว ผู้ใช้สามารถดาวน์โหลดได้จากเว็บไซต์ของ Oracle [24-6]

หากไม่สามารถอัพเดทได้ ผู้เชี่ยวชาญจากสถาบัน SANS แนะนำให้ผู้ใช้ปิดการทำงานของ Java ในเบราว์เซอร์ หรือใช้ปลั๊กอิน เช่น No-Script เพื่อเลือกอนุญาตให้ Java ทำงานได้เฉพาะในเว็บไซต์ที่กำหนด และหากไม่จำเป็นต้องใช้ความสามารถของ Java Runtime เวอร์ชัน 7 อาจดาวน์เกรดไปใช้ Java Runtime เวอร์ชัน 6 ที่อัพเดทล่าสุดแทนไปก่อนได้ [24-7]

บริษัท Apple ได้ปล่อยแพทช์เพื่อแก้ไขช่องโหว่ของ Java ใน Mac OS X เมื่อวันที่ 16 ตุลาคม 2555 [24-8] โดยแพทช์ดังกล่าวนี้จะอัพเดทโปรแกรม Java SE 6 เป็นเวอร์ชัน 1.6.0_37 พร้อมทั้งตัดการสนับสนุน Java ในเบราว์เซอร์ Safari ทำให้ผู้ใช้ที่ต้องการใช้งาน Java ใน Safari จำเป็นต้องติดตั้งปลั๊กอิน Java เวอร์ชันที่พัฒนาโดยบริษัท Oracle เอง [24-9]

## อ้างอิง


[24-1] http://blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html

[24-2] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4681

[24-3] http://labs.alienvault.com/labs/index.php/2012/new-java-0day-exploited-in-the-wild/

[24-4] https://community.rapid7.com/community/metasploit/blog/2012/08/27/lets-start-the-week-with-a-new-java-0day

[24-5] http://www.oracle.com/technetwork/topics/security/alerts-086861.html

[24-6] http://www.oracle.com/technetwork/java/javase/downloads/index-jsp-138363.html

[24-7] https://isc.sans.edu/diary.html?storyid=13984

[24-8] http://support.apple.com/kb/DL1572

[24-9] http://thehackernews.com/2012/10/apple-update-removes-java-plugin-from.html


# 23. ระวังภัย Foxit Reader เวอร์ชันเก่ากว่า 5.4 มีช่องโหว่ DLL hijacking

**วันที่ประกาศ:** 12 กันยายน 2555
**ปรับปรุงล่าสุด:** 12 กันยายน 2555
**เรื่อง:** ระวังภัย Foxit Reader เวอร์ชันเก่ากว่า 5.4 มีช่องโหว่ DLL hijacking
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

Foxit Software ผู้พัฒนาโปรแกรม Foxit Reader ซึ่งใช้ในการอ่านไฟล์ PDF ได้แจ้งว่าในโปรแกรม Foxit Reader เวอร์ชันเก่ากว่า 5.4 มีช่องโหว่ DLL hijacking ซึ่งอนุญาตให้ผู้ไม่หวังดีโจมตีผ่านไฟล์ DLL ที่เป็นอันตรายได้ และแนะนำให้ผู้ใช้อัพเดทเป็นเวอร์ชันล่าสุด [25-1]

## ผลกระทบ

เมื่อโปรแกรม Foxit Reader เริ่มทำงาน จะมีการโหลดไฟล์ DLL เข้ามาประมวลผล แต่หากโปรแกรมพบว่ามีไฟล์ DLL ที่มีชื่อเดียวกันกับไฟล์ DLL ที่ต้องการโหลดอยู่ในไดเรกทอรีที่ไฟล์ PDF อยู่ โปรแกรมก็จะโหลดไฟล์ DLL นั้นเข้ามาประมวลผลแทนไฟล์จริง

ในการโจมตี ผู้ไม่หวังดีสามารถใช้วิธีการวางไฟล์ PDF และไฟล์ DLL อันตรายไว้ในที่เดียวกัน เช่น วางไฟล์ไว้ใน Shared Directory แล้วให้เครื่องของเหยื่อเข้ามาเปิดไฟล์นั้น [25-2] เมื่อเหยื่อเปิดไฟล์ดังกล่าว คำสั่งอันตรายที่อยู่ในไฟล์ DLL ก็จะถูกนำไปประมวลผลทันที

## ระบบที่ได้รับผลกระทบ

Foxit Reader for Windows เวอร์ชันเก่ากว่า 5.4

## ข้อแนะนำในการป้องกันและแก้ไข

Foxit Software ได้ออกโปรแกรม Foxit Reader เวอร์ชัน 5.4

ซึ่งแก้ไขปัญหาดังกล่าวแล้ว [25-3] ผู้ใช้สามารถดาวน์โหลดได้จากเว็บไซต์ของ Foxit Reader หรือหากผู้ใช้ติดตั้งโปรแกรม Foxit Reader ไว้ในเครื่องอยู่แล้ว สามารถอัพเดทให้เป็นเวอร์ชันล่าสุดได้ด้วยการคลิกที่เมนู Help เลือก Check for Updates Now

## อ้างอิง


[25-1] http://www.h-online.com/security/news/item/Foxit-Reader-5-4-fixes-DLL-hijacking-vulnerability-1703878.html

[25-2] http://www.foxitsoftware.com/Secure_PDF_Reader/security_bulletins.php#malicious

[25-3] https://www.foxitsoftware.com/company/press.php?action=view&page=201209052316.html


# 24. Blizzard Entertainment ถูกเจาะระบบ ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยด่วน

**วันที่ประกาศ:** 10 สิงหาคม 2555
**ปรับปรุงล่าสุด:** 10 สิงหาคม 2555
**เรื่อง:** Blizzard Entertainment ถูกเจาะระบบ ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยด่วน
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

Blizzard Entertainment เป็นบริษัทที่พัฒนาเกมคอมพิวเตอร์ โดยมีเกมที่ได้รับความนิยม เช่น WarCraft, StarCraft, Diablo เป็นต้น ดังรูปที่ 8 (2-1) ซึ่งหลายเกมสามารถเล่นออนไลน์ได้ผ่านระบบ Battle.Net


*รูปที่ 27.รูปที่ 8 (2-1) ตัวอย่างเกมของ Blizzard Entertainment*

เมื่อวันที่ 9 สิงหาคม 2555 Blizzard Entertainment ได้แจ้งว่าระบบภายในของ Net ถูกเข้าถึงโดยไม่ได้รับอนุญาต จากการตรวจสอบพบว่า ผู้ไม่หวังดีได้ข้อมูลอีเมลที่ใช้ในการเข้าสู่ระบบ Battle.Net ในทุกภูมิภาคของโลก ยกเว้นประเทศจีน นอกจากนี้ยังได้ข้อมูลบัญชีผู้ใช้ในเซิร์ฟเวอร์ North America ซึ่งมีข้อมูลของผู้เล่นในภูมิภาคต่างๆ เช่น North America, Latin America, Australia, New Zealand และ Southeast Asia รวมอยู่ด้วย โดยข้อมูลที่หลุดออกไปนั้นประกอบด้วยรหัสผ่านที่ถูกเข้ารหัสลับไว้ คำตอบของคำถามที่ใช้ในการกู้คืนรหัสผ่าน และข้อมูลการยืนยันตัวตนผ่านโทรศัพท์มือถือ เป็นต้น [2-1]


ทาง Blizzard Entertainment ให้ข้อมูลเพิ่มเติมว่า ได้ตรวจสอบพบว่ามีการการเจาะระบบได้ตั้งแต่วันที่ 4 สิงหาคม 2555 แล้ว แต่ต้องการตรวจสอบข้อมูลให้ชัดเจนก่อน จึงได้ประกาศแจ้งเตือนในวันที่ 9 สิงหาคม [2-2] อย่างไรก็ตาม ทาง Blizzard Entertainment ได้แจ้งว่า ข้อมูลบัตรเครดิตและข้อมูลการซื้อสินค้านั้นไม่ได้รับผลกระทบจากการถูกเจาะระบบครั้งนี้

## ผลกระทบ

เนื่องจากรหัสผ่านที่หลุดออกไปนั้นเป็นรหัสผ่านที่ถูกเข้ารหัสลับไว้ แต่ผู้ไม่หวังดีได้ข้อมูลคำตอบของคำถามที่ใช้ในการกู้คืนรหัสผ่านไปด้วย ดังนั้นผู้ใช้งานระบบ Battle.Net มีโอกาสที่จะถูกขโมยบัญชีผู้ใช้ จากการตอบคำถามที่ใช้ในการกู้คืนรหัสผ่านได้

## ระบบที่ได้รับผลกระทบ

ระบบ Battle.Net

## ข้อแนะนำในการป้องกันและแก้ไข

บริษัท Blizzard Entertainment ได้แนะนำให้ผู้ที่ใช้งานระบบ Battle.Net เปลี่ยนรหัสผ่านโดยด่วน พร้อมกันนี้ ได้ให้ข้อมูลเพิ่มเติมว่า จะพัฒนาระบบเพื่ออำนวยความสะดวกในการเปลี่ยนรหัสผ่านและคำถามที่ใช้ในการกู้คืนรหัสผ่าน รวมถึงจะอัพเดทซอฟต์แวร์ที่ใช้ในการยืนยันตัวตนผ่านโทรศัพท์มือถือในเร็วๆ นี้ อย่างไรก็ตาม ทางบริษัทยังคงเปิดใช้งานระบบการยืนยันตัวตนผ่านโทรศัพท์มือถือ และระบบกู้คืนรหัสผ่านโดยวิธีการตอบคำถามที่ใช้ในการกู้คืนรหัสผ่านตามปกติ ถึงแม้ข้อมูลดังกล่าวจะถูกผู้ไม่หวังดีเข้าถึงได้แล้วก็ตาม

## อ้างอิง


[1-1] http://us.blizzard.com/en-us/company/press/pressreleases.html?id=6940026

[1-2] http://us.battle.net/support/en/article/important-security-update-faq

# 25. ระวังภัยช่องโหว่ใน Internet Explorer ผู้โจมตีสามารถทำ Remote Code Execution ได้ (CVE-2012-4969)

**วันที่ประกาศ:** 18 กันยายน 2555
**ปรับปรุงล่าสุด:** 25 กันยายน 2555
**เรื่อง:** ระวังภัย ช่องโหว่ใน Internet Explorer ผู้โจมตีสามารถทำ Remote Code Execution ได้ (CVE-2012-4969)
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

วันที่ 14 กันยายน 2555 ที่ผ่านมา Eric Romang ที่ปรึกษาด้านความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ได้ค้นพบช่องโหว่ของโปรแกรม Internet Explorer ซึ่งช่องโหว่นี้เกิดจาก Object หนึ่งที่ใช้ในขณะแสดงผลของโค้ดภาษา HTML ถูกลบออกจากหน่วยความจำ และในเวลาต่อมา Object นั้นถูกเรียกใช้อีกครั้ง ทำให้เกิดสภาวะ use-after-free ซึ่งทำให้โปรแกรมเกิดการทำงานผิดพลาด หลังจากการค้นพบ Romang ได้ส่งข้อมูลให้ผู้เชี่ยวชาญอื่น ๆ ช่วยยืนยันว่าข้อมูลที่พบเป็นช่องโหว่จริง [26-1]

ต่อมาในวันที่ 16 กันยายน 2555 ช่องโหว่นี้ได้รับการยืนยันจาก @binjo ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ดังนั้น Romang จึงได้เปิดเผยข้อมูลช่องโหว่ดังกล่าวต่อสาธารณะผ่าน Blog ของตนเอง [26-2]

วันที่ 17 กันยายน 2555 ทีมพัฒนา Metasploit ซึ่งเป็นเครื่องมือที่ใช้ในการทดสอบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ ได้อัพเดทเครื่องมือที่ใช้โจมตีช่องโหว่นี้เข้าเป็นส่วนหนึ่งของ Metasploit

## ผลกระทบ

ผู้โจมตีสามารถสร้างเว็บไซต์อันตรายแล้วหลอกให้เหยื่อเข้าไปยังเว็บไซต์ดังกล่าวผ่านโปรแกรม Internet Explorer ซึ่งอาจทำให้ถูกผู้โจมตีสามารถสั่งประมวลผลคำสั่งอันตรายจากระยะไกล (Remote Code Execution) ด้วยสิทธิในการทำงานของผู้ใช้ที่ล็อกอินได้

## ระบบที่ได้รับผลกระทบ

Internet Explorer เวอร์ชัน 6, 7, 8 และ 9 ที่ติดตั้งบนระบบปฏิบัติการ WindowsXP, Vista และ 7

## ข้อแนะนำในการป้องกันและแก้ไข

Microsoft ได้เผยแพร่แพทช์ KB2744842 เมื่อวันศุกร์ที่ 21 กันยายน 2555 ผู้ใช้งานสามารถติดตั้งได้ผ่านทาง Windows Update หรือดาวน์โหลดได้จากเว็บไซต์ของ Microsoft [26-3]

## อ้างอิง


[26-1] http://eromang.zataz.com/2012/09/17/microsoft-internet-explorer-execcommand-vulnerability-metasploit-demo/

[26-2] http://eromang.zataz.com/2012/09/16/zero-day-season-is-really-not-over-yet/

[26-3] http://technet.microsoft.com/en-us/security/bulletin/ms12-063




# 26. ระวังภัยโปรแกรม phpMyAdmin รุ่น 3.5.2.2 อาจมี Backdoor ฝังอยู่ (CVE-2012-5159)

**วันที่ประกาศ:** 27 กันยายน 2555
**ปรับปรุงล่าสุด:** 27 กันยายน 2555
**เรื่อง:** ระวังภัย โปรแกรม phpMyAdmin รุ่น 3.5.2.2 อาจมี Backdoor ฝังอยู่ (CVE-2012-5159)
**ประเภทภัยคุกคาม:** Malicious Code

## ข้อมูลทั่วไป

โปรแกรม phpMyAdmin เป็นโปรแกรมสำหรับจัดการฐานข้อมูล MySQL ที่นิยมใช้กันมาก ตัวโปรแกรมเขียนขึ้นด้วยภาษา php และใช้ติดตั้งในเครื่องแม่ข่ายเว็บที่สามารถเชื่อมต่อกับฐานข้อมูล MySQL ที่ต้องการจัดการได้ ผู้พัฒนา phpMyAdmin ได้ใช้ระบบของ Sourceforge เป็นสื่อกลางในการเผยแพร่โปรแกรม [27-1] ภายใต้ลิขสิทธิ์แบบ GPLv2 [27-2]

ในวันที่ 25 กันยายน 2555 มีการประกาศจาก Sourceforge ว่า พบ Backdoor ในสำเนาของ phpMyAdmin รุ่น 3.5.2.2 ในเครื่องแม่ข่ายเครื่องหนึ่งของ Sourceforge ที่ตั้งอยู่ในประเทศเกาหลี ซึ่งหลังจากพบเหตุดังกล่าว เครื่องแม่ข่ายที่มีปัญหาก็ได้ถูกระงับการให้บริการทันที แต่จากการตรวจสอบของ Sourceforge เอง พบว่ามีผู้ดาวน์โหลด phpMyAdmin สำเนาที่มี Backdoor นี้ออกไปจากเครื่องแม่ข่ายดังกล่าวไม่น้อยกว่า 400 ครั้ง ก่อนที่ Sourceforge จะปิดการให้บริการของเครื่องแม่ข่ายนี้ไป [27-3]

Backdoor ดังกล่าวพบในไฟล์ชื่อ server_sync.php ซึ่งไม่มีอยู่ในสำเนาของ phpMyAdmin ที่ถูกต้อง โดยไฟล์ดังกล่าวจะรับค่าใดๆ ผ่าน POST Method แล้วนำมาประมวลผลในระดับระบบปฏิบัติการ ซึ่งเป็นการเปิดช่องให้ผู้ไม่ประสงค์ดีสามารถโจมตีเครื่องแม่ข่ายที่ติดตั้ง phpMyAdmin ที่มี Backdoor นี้ในรูปแบบ Remote Command Execution ได้ โดยไม่ต้องยืนยันตัวตนก่อน [27-4]

## ผลกระทบ

ผู้ไม่ประสงค์ดีสามารถประมวลผลคำสั่งใดๆ ที่เป็นคำสั่งในระบบปฏิบัติการของเครื่องแม่ข่ายเป้าหมาย ในสิทธิระดับเดียวกับสิทธิของ Web Server Process ได้

## ระบบที่ได้รับผลกระทบ

เครื่องแม่ข่ายที่ติดตั้ง phpMyAdmin สำเนาที่มี Backdoor ติดตั้งอยู่

## ข้อแนะนำในการป้องกันและแก้ไข

ปัจจุบันนี้ เครื่องแม่ข่ายของ Sourceforge ในประเทศเกาหลีที่มีปัญหาได้ถูกระงับการให้บริการไปแล้ว และ Sourceforge เองได้ระบุว่า โปรแกรม phpMyAdmin รุ่น 3.5.2.2 ที่เผยแพร่ผ่านเครื่องแม่ข่ายเครื่องอื่นของ Sourceforge มีความมั่นคงปลอดภัย ส่วนผู้พัฒนาโปรแกรม phpMyAdmin ก็ได้ระบุว่าสำหรับผู้ที่ใช้งาน phpMyAdmin รุ่นดังกล่าวอยู่ ให้ตรวจหาว่ามีไฟล์ server_sync.php อยู่หรือไม่ หากพบว่ามีไฟล์ดังกล่าวแสดงว่า phpMyAdmin ที่ใช้งานอยู่เป็นสำเนาที่มี Backdoor อยู่ ควรทำการดาวน์โหลดโปรแกรม phpMyAdmin มาติดตั้งใหม่โดยด่วน [27-5]

## อ้างอิง


[27-1] http://sourceforge.net/projects/phpmyadmin/files/

[27-2] http://www.phpmyadmin.net/home_page/license.php

[27-3] http://sourceforge.net/blog/phpmyadmin-back-door

[27-4] http://arstechnica.com/security/2012/09/questions-abound-as-malicious-phpmyadmin-backdoor-found-on-sourceforge-site/

[27-5] http://www.phpmyadmin.net/home_page/security/PMASA-2012-5.php

# 27. ระวังภัยช่องโหว่ในระบบปฏิบัติการ Android ผู้ไม่หวังดีสามารถทำ Remote Factory Reset ได้

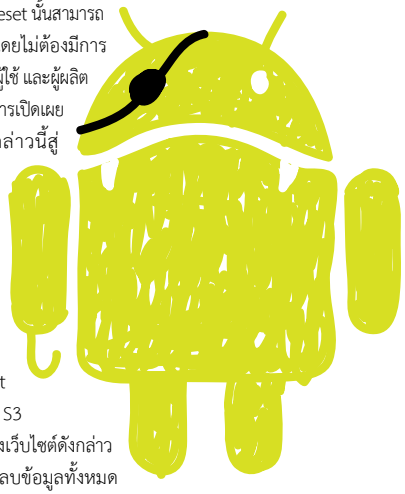
**วันที่ประกาศ:** 26 กันยายน 2555
**ปรับปรุงล่าสุด:** 26 กันยายน 2555
**เรื่อง:** ระวังภัย ช่องโหว่ในระบบปฏิบัติการ Android ผู้ไม่หวังดีสามารถทำ Remote Factory Reset ได้
**ประเภทภัยคุกคาม:** Malicious Code

## ข้อมูลทั่วไป

USSD หรือ Unstructured Supplementary Service Data เป็นโพรโทคอลที่โทรศัพท์มือถือใช้ในการส่งข้อมูลเพื่อติดต่อกับผู้ให้บริการในเครือข่าย GSM เช่น สมัครใช้บริการเสริม หรือตรวจสอบยอดเงินคงเหลือ เป็นต้น รูปแบบของ USSD โดยทั่วไปจะประกอบด้วยเครื่องหมาย * # และตัวเลขผสมกัน เช่น *123# เป็นต้น ในโทรศัพท์มือถือบางรุ่นจะมี USSD เพื่อใช้ในการเข้าถึงฟังก์ชั่นพิเศษของโทรศัพท์ เช่น กด *#06# เพื่อตรวจสอบหมายเลข IMEI ของเครื่อง หรือลบข้อมูลทั้งหมดในเครื่องให้อยู่ในสภาพที่ออกมาจากโรงงาน (Factory Reset) เป็นต้น ซึ่งในบางคำสั่ง จะทำงานทันทีที่กดตัวอักษรสุดท้ายเสร็จ โดยไม่จำเป็นต้องกดปุ่มโทรออกแต่อย่างใด [3-1]

ในงาน Ekoparty Security Conference นักวิจัยจาก Technical University Berlin ได้สาธิตช่องโหว่ของ USSD ใน Galaxy S3 ซึ่งอนุญาตให้ผู้ไม่หวังดีสามารถลบข้อมูลของเครื่องจากระยะไกลได้ (Remote Factory Reset) สาเหตุของช่องโหว่ดังกล่าวนี้เกิดจาก

1. แอปพลิเคชัน Dialer (Phone.apk) ของระบบปฏิบัติการ Android ซึ่งใช้ในการโทรศัพท์ จะทำการเปิด URI ที่ขึ้นต้นด้วย tel: โดยอัตโนมัติ แต่โดยปกติแล้วจะยังไม่ประมวลผลคำสั่งดังกล่าว
2. โปรแกรม Dialer ของผู้ผลิตบางราย (เช่น Samsung) ถูกตั้งค่าให้ประมวลผล USSD โดยอัตโนมัติ ซึ่งนำไปสู่การประมวลผลคำสั่งอันตรายได้
3. คำสั่ง USSD ที่เป็นอันตรายต่อระบบ เช่น การทำ Factory Reset นั้นสามารถทำงานได้โดยไม่ต้องมีการยืนยันจากผู้ใช้ และผู้ผลิตบางรายมีการเปิดเผยคำสั่งดังกล่าวนี้สู่สาธารณะ



นักวิจัยได้สาธิตการเปิดเว็บไซต์ที่มีแท็ก <iframe> ซึ่งภายในบรรจุโค้ด USSD สำหรับทำ Factory Reset ของเครื่อง Galaxy S3 ไว้ เมื่อผู้ใช้เข้าไปยังเว็บไซต์ดังกล่าว เครื่องก็จะทำการลบข้อมูลทั้งหมดเพื่อกลับไปสู่สภาพเดิมที่ออกมาจากโรงงานทันที วิดีโอสาธิตการโจมตีดังกล่าวสามารถดูได้จาก YouTube [3-2]

## ผลกระทบ

ผู้ไม่หวังดีสามารถสั่งลบข้อมูลในเครื่องของเหยื่อ ด้วยการหลอกให้เข้าไปยังเว็บไซต์ที่มีคำสั่งอันตราย หรือส่งคำสั่งดังกล่าวผ่านทาง QR Code, NFC หรือ Push Message ได้ [3-3]

## ระบบที่ได้รับผลกระทบ

ปัจจุบันมีรายงานว่ามีเพียงอุปกรณ์ที่ใช้งานระบบปฏิบัติการ Android ของ Samsung ที่ใช้ TouchWiz UI เท่านั้นที่มีช่องโหว่ Remote Factory Reset โดยนอกจาก Galaxy S3 แล้ว ผู้ใช้ Galaxy Beam, Galaxy S Advance, Galaxy Ace, และ Galaxy S II ได้แจ้งว่ามีช่องโหว่ดังกล่าวด้วย และจากข้อมูลใน XDA-Developers พบว่า โทรศัพท์มือถือของ HTC ก็มีช่องโหว่ดังกล่าวนี้ด้วยเช่นกัน แต่ยังไม่มีข้อมูลว่าสามารถทำ Factory Reset ได้ [3-4]

สำหรับเครื่องที่ใช้ระบบปฏิบัติการ Android ที่มาจาก Google โดยตรง เช่น Galaxy Nexus เมื่อเข้าไปยังหน้าเว็บไซต์ที่มีโค้ดอันตรายอยู่ จะแสดง USSD ในโปรแกรม Dialer แต่จะไม่ประมวลผลคำสั่ง USSD นั้นโดยอัตโนมัติ อีกทั้งมีผู้ใช้งานบางรายให้ข้อมูลเพิ่มเติมว่า โทรศัพท์มือถือที่ถูกติดตั้ง TouchWiz UI มาจากโรงงาน แต่นำมาติดตั้ง Custom Rom ที่พัฒนามาจาก Rom ของ Google โดยตรง เช่น CyanogenMod นั้นไม่มีปัญหาดังกล่าว [3-5]

นอกจากนี้ ยังมีรายงานเพิ่มเติมว่า แอปพลิเคชันประเภท Dialer บางตัวใน Play Store เช่น exDialer มีช่องโหว่ประมวลผล USSD โดยอัตโนมัติด้วยเช่นกัน

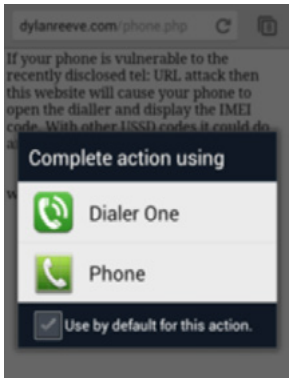
## ข้อแนะนำในการป้องกันและแก้ไข

ยังไม่มีแถลงการณ์จาก Samsung เกี่ยวกับช่องโหว่นี้ แต่มีรายงานจากผู้ใช้ Galaxy S3 ใน Forum ของ XDA-Developers ว่า Firmware ล่าสุดของ Galaxy S3 ได้แก้ไขปัญหานี้แล้ว [3-6] อย่างไรก็ตาม สำหรับผู้ใช้โทรศัพท์รุ่นอื่น ควรตรวจสอบข้อมูลกับศูนย์บริการอีกครั้งเพื่อความมั่นคงปลอดภัย

นาย Dylan Reeve ได้วิเคราะห์ช่องโหว่ดังกล่าว และได้ทำ หน้าเว็บไซต์สำหรับทดสอบช่องโหว่ดังกล่าวนี้ โดย หากผู้ใช้โทรศัพท์มือถือเข้าไปยังลิงก์ดังกล่าว แล้วพบว่าแอปพลิเคชัน Dialer แสดงหมายเลข IMEI ของเครื่องขึ้นมา แสดงว่าเครื่องที่ใช้งานอยู่นั้นมีช่องโหว่

อย่างไรก็ตาม เนื่องจากสาเหตุหลักของช่องโหว่ดังกล่าวนี้เกิดจากแอปพลิเคชัน Dialer ทำการประมวลผลคำสั่ง USSD โดยอัตโนมัติ วิธีแก้ปัญหาแบบชั่วคราวในขณะที่ยังไม่มีแพทช์มีดังนี้

1. ติดตั้งแอปพลิชัน Dialer เพิ่มเติม เพื่อใช้งานแทนแอปพลิเคชันที่มากับ Firmware อย่างไรก็ตาม การแก้ปัญหาด้วยวิธีนี้ ผู้ใช้ต้องแน่ใจว่าแอปพลิเคชันนั้นจะไม่ประมวลผลคำสั่ง USSD โดยอัตโนมัติ
2. ติดตั้งแอปพลิชัน Dialer เพิ่มเติม แต่ไม่ต้องตั้งค่าให้ใช้โปรแกรมใดเป็นค่า Default ของเครื่อง ซึ่งวิธีการดังกล่าวนี้จะทำให้เมื่อผู้ใช้เปิดเว็บที่มีโค้ด tel: อยู่ แล้วโปรแกรมต้องการโทรออกหรือประมวลผล USSD จะปรากฏหน้าจอให้ผู้ใช้เลือกว่าต้องการโทรออกโดยใช้แอปพลิเคชันใด ซึ่งผู้ใช้สามารถกดยกเลิกการโทรออกได้ อย่างไรก็ตาม การใช้งานวิธีนี้มีข้อเสียคือจำเป็นต้องเลือกโปรแกรมสำหรับใช้โทรออกทุกครั้ง [3-7] ดังรูปที่




*รูปที่ 28.รูปที่ 9 (3-1) หน้าจอการเลือกโปรแกรมสำหรับใช้โทรออก (ที่มา Dylan Reeve)*

3. ติดตั้ง Opera Mobile และใช้เป็นเบราว์เซอร์หลักของเครื่อง เนื่องจากจะไม่แสดงข้อมูลใน <iframe> โดยอัตโนมัติ ดังรูปที่


*รูปที่ 29.รูปที่ 10 (3-2) Opera Mobile ไม่แสดงผลข้อมูลใน <iframe>*

## อ้างอิง


[3-1] http://www.etsi.org/deliver/etsi_gts/02/0290/05.01.00_60/gsmts_0290v050100p.pdf

[3-2] http://www.youtube.com/watch?v=Q2-0B04HPhs

[3-3] http://www.zdnet.com/samsung-galaxy-s3-vulnerable-to-remote-malicious-reset-7000004771/

[3-4] http://forum.xda-developers.com/showthread.php?t=1904629

[3-5] http://techcrunch.com/2012/09/25/got-touchwiz-some-samsung-smartphones-can-be-totally-wiped-by-clicking-a-link/

[3-6] http://forum.xda-developers.com/showpost.php?p=31998672&postcount=33

[3-7] http://dylanreeve.posterous.com/remote-ussd-attack


# 28. Adobe ปล่อย CRL ยกเลิก Certificate ที่ถูกใช้ Sign มัลแวร์

**วันที่ประกาศ:** 5 ตุลาคม 2555
**ปรับปรุงล่าสุด:** 5 ตุลาคม 2555
**เรื่อง:** Adobe ปล่อย CRL ยกเลิก Certificate ที่ถูกใช้ Sign มัลแวร์
**ประเภทภัยคุกคาม:** Malicious Code

## ข้อมูลทั่วไป

เมื่อวันที่ 27 กันยายน 2555 Adobe ได้ประกาศแจ้งเตือนใน Blog ของบริษัทว่าได้ค้นพบมัลแวร์ที่ถูก Sign โดยใช้ Digital Certificate ของ Adobe จากการตรวจสอบพบว่ามัลแวร์ดังกล่าวนี้ถูก Sign โดยเซิร์ฟเวอร์ที่ใช้สำหรับ Sign โค้ดของโปรแกรม ซึ่งถูกผู้ไม่หวังดีเข้าไปควบคุม (Compromised) [28-1]

## ผลกระทบ

Microsoft ได้ตรวจสอบมัลแวร์ที่ถูก Sign โดยใช้ Certificate ของ Adobe โดยระบุชื่อของมัลแวร์ดังกล่าวนี้ว่า Win32/Adbposer พร้อมให้ข้อมูลเพิ่มเติมว่า จุดประสงค์หลักของผู้สร้างมัลแวร์ดังกล่าวนี้คือการหลบเลี่ยงการตรวจจับของโปรแกรมแอนตี้ไวรัส เนื่องจากโปรแกรมแอนตี้ไวรัสโดยส่วนใหญ่จะถูกออกแบบมาเพื่อให้ละเว้นการ ตรวจสอบโปรแกรมที่ถูก Sign โดยใช้ Certificate ของผู้พัฒนาที่เชื่อถือได้ (Trusted) เช่น Certificate ของ Adobe

## ข้อมูลของมัลแวร์ที่พบ มีดังนี้ [28-2]

PwDump7.exe

SHA1: c615a284e5f3f41cf829bbb939f2503b39349c8d

Signature timestamp: Thursday, July 26, 2012 8:44:40 PM PDT (GMT -7:00)

Detected as PWS:Win32/Adbposer.A

libeay.dll

SHA1: 934543f9ecc28ebefbd202c8e98833c36831ea75

Signature timestamp: Thursday, July 26, 2012 8:44:13 PM PDT (GMT -7:00)

Detected as PWS:Win32/Adbposer.A.dll

myGeeksmail.dll

SHA1: fecb579abfbc74f7ded61169214349d203a34378

Signature timestamp: Wednesday, July 25, 2012 8:48:59 PM (GMT -7:00)

Detected as Trojan:Win32/Adbposer.B

ผู้ใช้งานมีโอกาสเสี่ยงที่จะถูกโจมตีจากมัลแวร์ที่ถูก Sign โดยใช้ Certificate ดังกล่าว เนื่องจากโปรแกรมโปรแกรมแอนตี้ไวรัสจะไม่ตรวจสอบโปรแกรมดังกล่าวเพราะเชื่อ ถือว่าไม่ใช่โปรแกรมที่เป็นอันตราย

## ระบบที่ได้รับผลกระทบ

ระบบปฏิบัติการ Windows

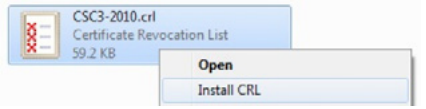
## ข้อแนะนำในการป้องกันและแก้ไข

เมื่อวันที่ 4 ตุลาคม 2555 Adobe ได้ปล่อย Certificate Revocation List เพื่อเพิกถอน (Revoke) Certificate ของซอฟต์แวร์ที่ถูก Sign หลังจากวันที่ 10 กรกฎาคม 2555 (00:00 GMT) [28-3] โดยผู้ใช้สามารถดาวน์โหลด CRL ดังกล่าวได้จาก http://csc3-2010-crl.verisign.com/CSC3-2010.crl

ข้อมูลของ Certificate ดังกล่าวมีดังนี้

- sha1RSA certificate
- Issued to Adobe Systems Incorporated
- Issued by VeriSign Class 3 Code Signing 2010 CA
- Serial Number: 15 e5 ac 0a 48 70 63 71 8e 39 da 52 30 1a 04 88
- sha1 Thumbprint: fd f0 1d d3 f3 7c 66 ac 4c 77 9d 92 62 3c 77 81 4a 07 fe 4c
- Valid from December 14, 2010 5:00 PM PST (GMT -8:00) to December 14, 2012 4:59:59 PM PST (GMT -8:00)

การติดตั้ง CRL เข้าไปในระบบ ทำได้โดยการคลิกขวาที่ไฟล์ CSC3-2010.crl แล้วเลือก Install CRL ดังรูปที่ 30 (28-1)




*รูปที่ 30.รูปที่ 30 (28-1) การติดตั้ง CRL*

อย่างไรก็ตาม หลังจากการติดตั้ง Certificate ดังกล่าวนี้ ระบบปฏิบัติการจะแจ้งว่าโปรแกรมของ Adobe ที่ถูก Sign โดยใช้ Certificate ดังกล่าวเป็นโปรแกรมที่ไม่น่าเชื่อถือ แต่ยังสามารถติดตั้งและใช้งานได้ตามปกติ ซึ่งทาง Adobe จะปล่อยอัพเดทของโปรแกรมดังกล่าวที่ถูก Sign โดยใช้ Certificate ใหม่ออกมาในภายหลัง

## อ้างอิง


[28-1] http://blogs.adobe.com/asset/2012/09/inappropriate-use-of-adobe-code-signing-certificate.html

[28-2] http://blogs.technet.com/b/mmpc/archive/2012/10/03/malware-signed-with-the-adobe-code-signing-certificate.aspx

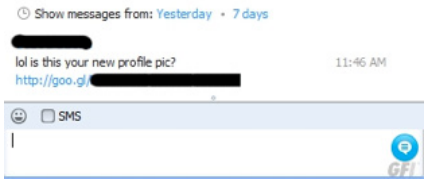
[28-3] http://www.adobe.com/support/security/advisories/apsa12-01.html

# 29. ระวังภัยมัลแวร์ใน Skype ล็อคไฟล์ในเครื่อง

**วันที่ประกาศ:** 13 ตุลาคม 2555
**ปรับปรุงล่าสุด:** 13 ตุลาคม 2555
**เรื่อง:** ระวังภัย มัลแวร์ใน Skype ล็อคไฟล์ในเครื่อง
**ประเภทภัยคุกคาม:** Malicious Code

## ข้อมูลทั่วไป

GFI Labs หน่วยงานที่วิจัยเรื่องภัยคุกคามทางคอมพิวเตอร์ ได้รายงานการค้นพบมัลแวร์ที่เผยแพร่ผ่านโปรแกรม Skype [29-1] โดยผู้ใช้จะได้รับข้อความพร้อมลิงก์สำหรับดาวน์โหลดไฟล์ ดังรูปที่ 31 (29-1)



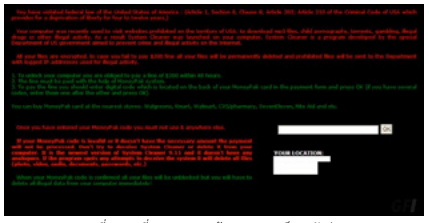

*รูปที่ 31.รูปที่ 31 (29-1) ข้อความและลิงก์สำหรับดาวน์โหลดมัลแวร์*

เมื่อผู้ใช้คลิกที่ลิงก์ดังกล่าว จะนำไปสู่การดาวน์โหลดไฟล์ .zip ซึ่งภายในบรรจุไฟล์ .exe ที่มีไอคอนของโปรแกรม Skype ดังรูปที่ 32 (29-2) ซึ่งเป็นไฟล์ของมัลแวร์


*รูปที่ 32.รูปที่ 32 (29-2) ไฟล์ของมัลแวร์*

## ผลกระทบ

หากผู้ใช้สั่งรันไฟล์ .exe ดังกล่าว มัลแวร์จะเข้ารหัสลับ (Encrypt) ไฟล์ในเครื่องของผู้ใช้ และแสดงหน้าจอให้ผู้ใช้จ่ายเงิน $200 เพื่อปลดล็อครหัสผ่านของไฟล์นั้นๆ ดังรูปที่ 33 (29-3)



*รูปที่ 33.รูปที่ 33 (29-3) หน้าจอการปลดล็อครหัสผ่าน*

## ระบบที่ได้รับผลกระทบ

ระบบปฏิบัติการ Windows ที่ติดตั้งโปรแกรม Skype

## ข้อแนะนำในการป้องกันและแก้ไข

หน่วยงาน CERT ของประเทศโปแลนด์ ได้รายงานว่ามัลแวร์ดังกล่าวเป็น Worm ชื่อ Dorkbot ซึ่งโปรแกรมแอนตี้ไวรัสส่วนใหญ่สามารถตรวจจับและกำจัดมัลแวร์นี้ได้ [29-2]

วิธีการป้องกันตัวจากการโจมตีด้วยวิธีดังกล่าว ผู้ใช้ไม่ควรคลิกลิงก์ที่น่าสงสัย และควรอัพเดทฐานข้อมูลของโปรแกรมแอนตี้ไวรัสให้เป็นเวอร์ชันล่าสุดอยู่เสมอ

หมายเหตุ: รูปประกอบทั้งหมดจาก GFI Labs

## อ้างอิง


[29-1] http://www.gfi.com/blog/skype-users-targeted-with-ransomware-and-click-fraud/

[29-2] http://www.cert.pl/news/6434/langswitch_lang/en

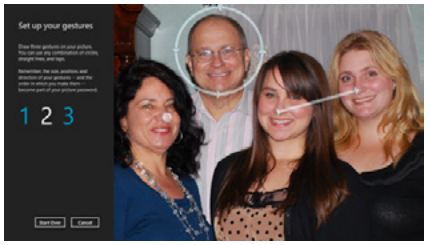



# 30. ระวังภัย Windows 8 เก็บข้อมูลการ Login ด้วย Picture Password เป็น Plain Text

**วันที่ประกาศ:** 13 ตุลาคม 2555
**ปรับปรุงล่าสุด:** 13 ตุลาคม 2555
**เรื่อง:** ระวังภัย Windows 8 เก็บข้อมูลการ Login ด้วย Picture Password เป็น Plain Text
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

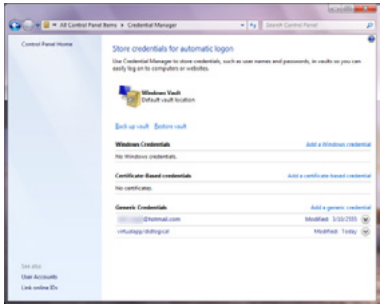
Windows 8 มีความสามารถใหม่ที่เรียกว่า Picture Password ซึ่งเป็นการ Login โดยการแตะรูปภาพในตำแหน่งที่กำหนด [30-1] ดังรูปที่ 34 (30-1) ซึ่งผู้ใช้สามารถศึกษาข้อมูลเพิ่มเติมได้จาก วิดีโอของ Microsoft




*รูปที่ 34.รูปที่ 34 (30-1) ระบบ Picture Password (ที่มา Microsoft)*

บริษัท Passcape ซึ่งพัฒนาโปรแกรมรักษาความมั่นคงปลอดภัย ได้ค้นพบช่องโหว่ของระบบการ Login ด้วยวิธีดังกล่าว [30-2] โดยสาเหตุของช่องโหว่ เกิดจากเมื่อผู้ใช้ต้องการใช้งานการ Login แบบ Picture Password จำเป็นต้องสร้าง User Account พร้อมตั้งรหัสผ่านเป็นแบบข้อความธรรมดาก่อน จากนั้นจึงจะสามารถตั้งค่าการ Login ด้วย Picture Password ได้ แต่หลังจากที่ผู้ใช้ตั้งค่าการ Login ด้วย Picture Password แล้ว ระบบจะเก็บรหัสผ่านที่เป็นข้อความธรรมดานั้นโดยใช้การเข้ารหัสลับ (Encrypt) แบบ AES ไว้ใน Windows Vault

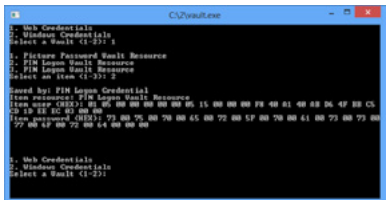
Windows Vault เป็นความสามารถที่ถูกพัฒนาขึ้นมาใน Windows 7 มีจุดประสงค์เพื่อใช้สำหรับเก็บชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการเข้าใช้งานเซิร์ฟเวอร์ เว็บไซต์ หรือโปรแกรมอื่นๆ โดยอัตโนมัติ [30-3] ดังรูปที่ 35 (30-2)




*รูปที่ 35.รูปที่ 35 (30-2) ระบบ Windows Vault ใน Windows 7*

## ผลกระทบ

ถึงแม้รหัสผ่านจะถูก Encrypt ไว้ แต่ผู้ใช้ในเครื่องที่มีสิทธิของผู้ดูแลระบบ (Administrator) ก็ยังสามารถเปิดดูรหัสผ่านแบบ Plain Text ของผู้ใช้ในระบบได้ ดังรูปที่ 36 (30-3) ซึ่งเป็นโปรแกรม Windows Password Recovery ของบริษัท Passcape




*รูปที่ 36.รูปที่ 36 (30-3) โปรแกรม Windows Password Recovery ของบริษัท Passcape (ที่มา Passcape)*

## ระบบที่ได้รับผลกระทบ

ระบบปฏิบัติการ Windows 8 ที่ใช้การ Login แบบ Picture Passwords

## ข้อแนะนำในการป้องกันและแก้ไข

บริษัท Passcape แนะนำว่า ผู้ใช้งาน Windows 8 ไม่ควรตั้งค่าการ Login ด้วย Picture Password จนกว่า Microsoft จะออกแพทช์เพื่อแก้ไขช่องโหว่ดังกล่าว

## อ้างอิง


[30-1] http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx

[30-2] http://www.passcape.com/index.php?section=blog&cmd=details&id=27&setLang=2

[30-3] http://www.neowin.net/news/main/09/03/07/windows-7-exploring-credential-manager-and-windows-vault


# 31. ระวังภัยโปรแกรม Atomymaxsite รุ่น 2.5 หรือต่ำกว่า มีช่องโหว่อัพโหลดไฟล์ใดๆ ได้โดยไม่มีการตรวจสอบ

**วันที่ประกาศ:** 17 ตุลาคม 2555
**ปรับปรุงล่าสุด:** 24 ตุลาคม 2555
**เรื่อง:** ระวังภัย โปรแกรม Atomymaxsite รุ่น 2.5 หรือต่ำกว่า มีช่องโหว่อัพโหลดไฟล์ใดๆ ได้โดยไม่มีการตรวจสอบ
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

โปรแกรม Atomymaxsite เป็นโปรแกรมสร้างเว็บไซต์สำเร็จรูปในรูปแบบ CMS ที่พัฒนาโดยนักพัฒนาชาวไทย ปัจจุบันมีผู้พัฒนาอยู่ 2 ค่าย คือ ในเว็บไซต์ Atomymaxsite [31-1] ระบุว่าพัฒนาโดยนายชัดสกร พิกุลทอง ผู้อำนวยการโรงเรียนบ้านผือ อำเภอชื่นชม จังหวัดมหาสารคาม และผู้ที่จะนำไปใช้งานจะต้องบริจาคเงินจำนวนหนึ่งผ่านบัญชีธนาคารที่ระบุใน เว็บไซต์ดังกล่าวก่อน จึงจะได้สิทธิ์ในการดาวน์โหลด โดยมีรุ่นล่าสุดคือ รุ่น 2.5 และในเว็บไซต์ Maxsite-board [31-2] ระบุว่าซอฟท์แวร์ Atomymaxsite เป็นซอฟต์แวร์ที่แจกจ่ายโดยไม่คิดมูลค่า (ตามข้อกำหนด GPL v3) ผ่าน Google Code [31-3] และมีรุ่นของซอฟต์แวร์ที่แตกต่างกันคือ 2.5.0, 2.5.1 และรุ่นล่าสุดคือ 2.5.2 ซึ่งคาดว่าทั้งหมด เป็นการปรับปรุงจากรุ่น 2.5 เดิมนั่นเอง

ในวันที่ 1 ตุลาคม 2555 ได้มีผู้โพสต์วิดีโอในเว็บไซต์ Youtube โดยใช้ภาษาต่างประเทศที่คาดว่าจะเป็นภาษาอาหรับ แสดงวิธีการโจมตีเว็บไซต์ที่ใช้ซอฟต์แวร์ Atomymaxsite รุ่น 2.5 โดยอาศัยช่องโหว่ Arbitrary file upload ของโมดูลที่ใช้เผยแพร่ผลงานวิชาการ ซึ่งช่องโหว่นี้ทำให้ผู้ไม่ประสงค์ดีสามารถอัพโหลดไฟล์ใดๆ เข้าสู่เครื่องแม่ข่ายได้โดยไม่มีการตรวจสอบชนิดของแฟ้มที่อัพโหลดแต่อย่าง ใด และไม่ต้องทำการยืนยันตัวตนก่อน

## ผลกระทบ

ผู้ไม่ประสงค์ดีสามารถอัพโหลดแฟ้มข้อมูลประเภท PHP Shell หรือแฟ้ม PHP ที่มีคำสั่งไม่พึงประสงค์เข้าไปในเครื่องแม่ข่ายเป้าหมาย และสามารถเรียกใช้งานคำสั่งดังกล่าว ในสิทธิระดับเดียวกับสิทธิของ Web Server Process ได้

## ระบบที่ได้รับผลกระทบ

เครื่องแม่ข่ายที่ติดตั้ง Atomymaxsite รุ่น 2.5 หรือต่ำกว่า

## ข้อแนะนำในการป้องกันและแก้ไข

จากการตรวจสอบข้อมูลเบื้องต้นจาก Source Code ของซอฟต์แวร์ Atomymaxsite รุ่น 2.5.0 และ 2.5.2 ที่ดาวน์โหลดมาจาก Google code พบว่ามีการเพิ่มการตรวจสอบชนิดของแฟ้มข้อมูลที่ผู้ใช้งานอัพโหลดในโมดูลที่ เป็นปัญหาดังกล่าวแล้ว โดยกำหนดให้แฟ้มข้อมูลที่สามารถอัพโหลดได้เป็นชนิด pdf, zip, doc, docx, ppt, pptx, xls, และ xlsx เท่านั้น ตั้งแต่รุ่น 2.5.0 และมีการเพิ่มการป้องกันการเรียกใช้แฟ้มที่ไม่ใช่รูปภาพจากโฟลเดอร์ /data ซึ่งใช้เก็บแฟ้มที่อัพโหลดเข้าเว็บไซต์ โดยใช้วิธีการเพิ่มแฟ้ม .htaccess ในโฟลเดอร์ดังกล่าว ทำให้ Atomymaxsite รุ่นที่มีการแจกจ่ายผ่าน Google code ไม่มีผลกระทบจากช่องโหว่ดังกล่าว ผู้ใช้งาน Atomymaxsite รุ่น 2.5 หรือต่ำกว่า จึงควรเปลี่ยนไปใช้งานรุ่นที่ไม่ได้รับผลกระทบตามที่ได้กล่าวข้างต้น

ในวันที่ 18 ตุลาคม 2555 ผู้พัฒนาโปรแกรม Atomymaxsite รุ่น 2.5 [31-4] ได้มีการแจ้งข้อมูลการอัพเดทซอฟต์แวร์เพื่อแก้ไขช่องโหว่ดังกล่าว [31-5][31-6] ซึ่งผู้ใช้งานควรรีบดำเนินการตรวจสอบการปรับปรุงซอฟต์แวร์ดังกล่าวเพื่อป้องกันการถูกโจมตี หรือหากยังไม่แน่ใจว่าเว็บไซต์ของท่านใช้งานซอฟต์แวร์รุ่นที่มีช่องโหว่ดังกล่าวหรือไม่ รวมถึงในกรณีที่ท่านต้องการสอบถามข้อมูลเพิ่มเติม ทางไทยเซิร์ตแนะนำให้ท่านปรึกษากับเว็บไซต์ผู้พัฒนาซอฟต์แวร์ที่ท่านดาวโหลดมาติดตั้งโดยตรง เพื่อป้องกันความผิดพลาดจากการอัพเดทซอฟต์แวร์ที่ผิดวิธี ซึ่งอาจทำให้เว็บไซต์ของท่านไม่สามารถเรียกใช้งานได้

## อ้างอิง


[31-1] http://maxtom.sytes.net

[31-2] http://board.maxsitepro.com/

[31-3] http://code.google.com/p/atommy-maxsite-2-5/

[31-4] http://maxtom.sytes.net

[31-5] http://maxtom.sytes.net/?name=webboard&file=read&id=798

[31-6] http://maxtom.sytes.net/?name=webboard&file=read&id=764


# 32. ระวังภัย ชิป Wifi ของ Broadcom รุ่น BCM4325 และ BCM4329 มีช่องโหว่ DoS

**วันที่ประกาศ:** 25 ตุลาคม 2555
**ปรับปรุงล่าสุด:** 25 ตุลาคม 2555
**เรื่อง:** ระวังภัย ชิป Wifi ของ Broadcom รุ่น BCM4325 และ BCM4329 มีช่องโหว่ DoS
**ประเภทภัยคุกคาม:** Denial of Service

## ข้อมูลทั่วไป

ศูนย์วิจัยด้านความมั่นคงปลอดภัยของ Core Security Technologies ได้ค้นพบช่องโหว่ในชิป Wifi ของ Broadcom รุ่น BCM4325 และ BCM4329 ซึ่งชิปทั้ง 2 รุ่นนี้ถูกนำไปใช้โทรศัพท์มือถือ แท็บเล็ต หรือแม้กระทั่งรถยนต์ สาเหตุของช่องโหว่ดังกล่าวเกิดจากเฟิร์มแวร์ของตัวชิปไม่มีการตรวจสอบข้อมูลที่ได้รับเข้ามา

## ผลกระทบ

ผู้ไม่หวังดีสามารถส่งข้อมูลบางอย่างมาที่เครื่องของเหยื่อเพื่อสั่งให้ชิป Wifi หยุดทำงาน (Denial of Service) หรืออาจสั่งให้ชิปไปอ่านข้อมูลในส่วนที่การทำงานปกติไม่สามารถอ่านได้ (Information Disclosure) ปัจจุบันมี Proof of Concept Code สำหรับโจมตีผ่านช่องโหว่ดังกล่าวเผยแพร่สู่สาธารณะแล้ว [32-1]

## ระบบที่ได้รับผลกระทบ

โทรศัพท์มือถือ, แท็บเล็ต และอุปกรณ์ที่ใช้ชิป Wifi ของ Broadcom รุ่น BCM4325 หรือ BCM4329 ดังนี้

- **BCM4325**
  - Apple iPhone 3GS
  - Apple iPod 2G

- HTC Touch Pro 2
- HTC Droid Incredible
- Samsung Spica
- Acer Liquid
- Motorola Devour
- รถยนต์ Ford Edge

- **BCM4329**
  - Apple iPhone 4
  - Apple iPhone 4 Verizon
  - Apple iPod 3G
  - Apple iPad Wi-Fi
  - Apple iPad 3G
  - Apple iPad 2
  - Apple TV 2G
  - Motorola Xoom
  - Motorola Droid X2
  - Motorola Atrix
  - Samsung Galaxy Tab
  - Samsung Galaxy S 4G
  - Samsung Nexus S
  - Samsung Stratosphere
  - Samsung Fascinate
  - HTC Nexus One
  - HTC Evo 4G
  - HTC ThunderBolt
  - HTC Droid Incredible 2
  - LG Revolution
  - Sony Ericsson Xperia Play
  - Pantech Breakout
  - Nokia Lumina 800
  - Kyocera Echo
  - Asus Transformer Prime
  - Malata ZPad

## ข้อแนะนำในการป้องกันและแก้ไข

บริษัท Broadcom ได้ทราบถึงปัญหานี้แล้ว และได้ชี้แจงว่าชิปจะหยุดการทำงานในระหว่างที่ผู้โจมตีส่งคำสั่งอันตรายมา ยังตัวชิป และจะกลับมาทำงานได้ตามปกติเมื่อผู้โจมตียกเลิกคำสั่งนั้น อย่างไรก็ตาม ในระหว่างที่ตัวชิปถูกขัดขวางการทำงานนั้น ระบบอื่นๆ ของโทรศัพท์มือถือหรือแท็บเล็ตยังสามารถทำงานได้ตามปกติ และการขัดขวางการทำงานของชิป Wifi ไม่มีผลต่อความมั่นคงปลอดภัยของข้อมูลของผู้ใช้งาน [32-2]

ทาง Broadcom ได้เผยแพร่แพทช์สำหรับแก้ไขช่องโหว่ของปัญหานี้แล้ว อย่างไรก็ตาม ผู้ใช้งานโทรศัพท์มือถือ แท็บเล็ตหรืออุปกรณ์ที่ใช้ชิป Wifi ดังกล่าวอาจต้องรอซอฟต์แวร์อัพเดทจากผู้ผลิตอุปกรณ์นั้นๆ

## อ้างอิง


[32-1] http://www.coresecurity.com/content/broadcom-input-validation-BCM4325-BCM4329

[32-2] http://www.zdnet.com/wi-fi-chips-in-phones-tablets-vulnerable-to-dos-attack-7000006352/




# 33. ระวังภัยช่องโหว่ Use-after-free ใน Mozilla Firefox/ Thunderbird เวอร์ชันต่ำกว่า 17.0

**วันที่ประกาศ:** 28 พฤศจิกายน 2555
**ปรับปรุงล่าสุด:** 28 พฤศจิกายน 2555
**เรื่อง:** ระวังภัย ช่องโหว่ Use-after-free ใน Mozilla Firefox/ Thunderbird เวอร์ชันต่ำกว่า 17.0
**ประเภทภัยคุกคาม:** Malicious Code, Denial-of-Service

## ข้อมูลทั่วไป

บริษัท VUPEN Security ได้รายงานช่องโหว่ในโปรแกรม Mozilla Firefox, Mozilla Thunderbird และ Mozilla SeaMonkey [33-1] โดยช่องโหว่ดังกล่าวนี้เกิดจากข้อผิดพลาด Use-after-free (เรียกใช้งานข้อมูลที่ถูกลบออกจากหน่วยความจำไปแล้ว) ในฟังก์ชั่น DocumentViewerImpl::-Show()

## ผลกระทบ

ผู้ไม่หวังดีสามารถสั่งประมวลผลคำสั่งอันตรายจากระยะไกลที่เครื่องของเหยื่อ หลังจากที่เหยื่อเข้าไปยังเว็บไซต์อันตรายที่มีโค้ดการโจมตีผ่านช่องโหว่ดังกล่าวอยู่

ระบบที่ได้รับผลกระทบ

- Mozilla Firefox เวอร์ชันต่ำกว่า 17.0
- Mozilla Firefox ESR เวอร์ชันต่ำกว่า 10.0.11
- Mozilla Thunderbird เวอร์ชันต่ำกว่า 17.0
- Mozilla Thunderbird ESR เวอร์ชันต่ำกว่า 10.0.11
- Mozilla SeaMonkey เวอร์ชันต่ำกว่า to 2.14

หมายเหตุ: Mozilla Firefox ESR และ Mozilla Thunderbird ESR เป็นเวอร์ชันที่จะได้รับการสนับสนุนทางเทคนิคยาวนานกว่าเวอร์ชันปกติ (Extended Support Release) สำหรับใช้ในหน่วยงานหรือองค์กรที่ต้องมีการดูแลระบบจำนวนมาก [33-2]

ข้อแนะนำในการป้องกันและแก้ไข

ผู้ใช้งานโปรแกรมที่ได้รับผลกระทบจากช่องโหว่ดังกล่าว ควรอัพเดตโปรแกรมให้เป็นเวอร์ชันล่าสุด

## อ้างอิง


[33-1] http://seclists.org/bugtraq/2012/Nov/93

[33-2] http://www.mozilla.org/en-US/firefox/organizations/

# 34. ระวังภัยไดรเวอร์เครื่องพิมพ์ของ Samsung และ Dell มี Backdoor Administrator Account

**วันที่ประกาศ:** 28 พฤศจิกายน 2555
**ปรับปรุงล่าสุด:** 28 พฤศจิกายน 2555
**เรื่อง:** ระวังภัย ไดรเวอร์เครื่องพิมพ์ของ Samsung และ Dell มี Backdoor Administrator Account
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

US-CERT แจ้งเตือนว่ามีการ hard-coded รหัสผ่านของผู้ใช้งานที่มีสิทธิ Administrator ไว้ในไดรเวอร์เครื่องพิมพ์ของ Samsung และเครื่องพิมพ์ของ Dell รุ่นที่ผลิตโดย Samsung ช่องโหว่ดังกล่าวนี้ส่งผลให้ผู้ไม่หวังดีสามารถเชื่อมต่อเข้ามาที่เครื่องพิมพ์ผ่านโพรโทคอล SNMP ได้ ถึงแม้จะมีการปิดการทำงานของ SNMP ใน Printer management utility แล้วก็ตาม [34-1]

## ผลกระทบ

ผู้ไม่หวังดีสามารถเชื่อมต่อจากระยะไกลเพื่อเข้ามาควบคุมเครื่องพิมพ์เหล่านี้ ได้โดยได้รับสิทธิของ Administrator ซึ่งทำให้สามารถแก้ไขค่าการทำงาน ดูข้อมูลสำคัญที่เป็นความลับ (เช่น การตั้งค่าการเชื่อมต่อระบบเครือข่าย หรือข้อมูลต่างๆ ที่ถูกส่งเข้ามายังเครื่องพิมพ์ ซึ่งอาจเป็นการสั่งพิมพ์เอกสารที่เป็นความลับ) นอกจากนี้ยังสามารถสั่งให้เครื่องพิมพ์ดังกล่าวประมวลผลคำสั่งที่เป็นอันตรายจากระยะไกลได้ (Remote code execution)

## ระบบที่ได้รับผลกระทบ

เครื่องพิมพ์ของ Samsung และ Dell ที่วางจำหน่ายก่อนวันที่ 31 ตุลาคม 2555

## ข้อแนะนำในการป้องกันและแก้ไข

Samsung แจ้งว่าเครื่องพิมพ์ที่จัดจำหน่ายหลังจากวันที่ 31 ตุลาคม 2555 ได้แก้ไขปัญหาดังกล่าวแล้ว และจะเผยแพร่แพทช์สำหรับแก้ไขปัญหาในเครื่องพิมพ์รุ่นก่อนหน้าภายในปีนี้

ระหว่างที่รอแพทช์ ผู้ใช้งานสามารถตั้งค่าการเชื่อมต่อให้เครื่องพิมพ์สามารถเชื่อมต่อได้จากเครือข่ายภายในเท่านั้น รวมถึงบล็อกการเชื่อมต่อแบบ SNMP จากเครือข่ายภายนอก

## อ้างอิง

[34-1] http://www.kb.cert.org/vuls/id/281284

# 35. ระวังภัย Instagram 3.1.2 ใน iOS มีช่องโหว่สวมรอยบัญชีผู้ใช้

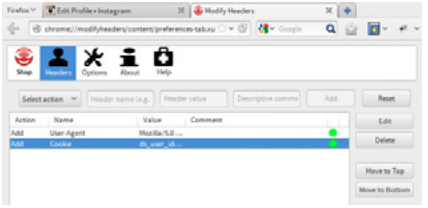
**วันที่ประกาศ:** 4 ธันวาคม 2555
**ปรับปรุงล่าสุด:** 4 ธันวาคม 2555
**เรื่อง:** ระวังภัย Instagram 3.1.2 ใน iOS มีช่องโหว่สวมรอยบัญชีผู้ใช้
**ประเภทภัยคุกคาม:** Intrusion

## ข้อมูลทั่วไป

นักวิจัยค้นพบช่องโหว่ในแอปพลิเคชัน Instagram เวอร์ชัน 3.1.2 ที่เผยแพร่เมื่อวันที่ 23 ตุลาคม 2555 โดยพบว่าแอปพลิเคชันดังกล่าวส่งข้อมูลการเข้าสู่ระบบหรือการแก้ไขข้อมูลของผู้ใช้ผ่านโพรโทคอล HTTPS แต่ข้อมูลในส่วนของการใช้งานอื่นๆ นั้นส่งผ่านโพรโทคอล HTTP โดยไม่มีการป้องกัน [35-1]


## ผลกระทบ

หากผู้ใช้งาน Instagram เชื่อมต่อเข้ากับเครือข่าย Wifi สาธารณะ อาจถูกผู้ไม่หวังดีใช้โปรแกรมประเภท Sniffer ในการดักรับข้อมูล หรืออาจถูกผู้ไม่หวังดีโจมตีด้วยวิธี Man-in-the-Middle เพื่อดักจับ Cookie และสวมรอยบัญชีผู้ใช้ รวมถึงอาจลบภาพของผู้ใช้งานได้ [35-2] ดังรูปที่ 37 (35-1)



*รูปที่ 37. รูปที่ 37 (35-1) ตัวอย่างการดักรับข้อมูล Cookie ของ Instagram (ที่มา reventlov.com)*

## ระบบที่ได้รับผลกระทบ

Instagram 3.1.2 ใน iOS

## ข้อแนะนำในการป้องกันและแก้ไข

นักวิจัยได้แจ้งช่องโหว่นี้ให้ทาง Instagram ทราบแล้ว ในระหว่างที่ Instagram กำลังแก้ไขช่องโหว่ดังกล่าว ผู้ใช้งาน iOS ไม่ควรเปิดใช้งาน Instagram ในขณะที่เชื่อมต่อกับเครือข่าย Wifi สาธารณะเพราะอาจถูกสวมรอยบัญชีผู้ใช้ได้ ควรใช้การเชื่อมต่อผ่าน Cellular Network เพื่อความมั่นคงปลอดภัย

## อ้างอิง

[35-1] http://reventlov.com/advisories/instagram-plain-text-media-disclosure-issue

[35-2] http://reventlov.com/advisories/instagram-session-riding-vulnerability

# 36. ระวังภัย แฮ็กเกอร์เผย 5 ช่องโหว่ 0-Day ใน MySQL

**วันที่ประกาศ:** 4 ธันวาคม 2555
**ปรับปรุงล่าสุด:** 4 ธันวาคม 2555
**เรื่อง:** ระวังภัย แฮ็กเกอร์เผย 5 ช่องโหว่ 0-Day ใน MySQL
**ประเภทภัยคุกคาม:** Intrusion, Denial of Service

## ข้อมูลทั่วไป

แฮ็กเกอร์ที่ใช้นามแฝงว่า Kingcope ได้เผยแพร่ช่องโหว่ 0-Day ของโปรแกรม MySQL ในระบบกระดานข่าวของเว็บไซต์ Full Disclosure โดยมีทั้งหมด 5 ช่องโหว่ดังนี้ [36-1]

1. CVE-2012-5611 — MySQL (Linux) Stack based buffer overrun PoC Zeroday
    - Stack-based buffer overflow อนุญาตให้ผู้ใช้ที่ได้รับสิทธิในการเข้าถึงระบบ สามารถสั่งประมวลผลคำสั่งอันตรายจากระยะไกล (Remote code execution) เพื่อได้รับสิทธิของคำสั่ง GRANT FILE
2. CVE-2012-5612 — MySQL (Linux) Heap Based Overrun PoC Zeroday
    - Heap-based buffer overflow อนุญาตให้ผู้ใช้ที่ได้รับสิทธิในการเข้าถึงระบบสามารถทำ Denial of Service (Memory corruption และ Crash) และอาจสั่งประมวลผลคำสั่งอันตรายจากระยะไกลได้ เช่นคำสั่ง (1) USE, (2) SHOW TABLES, (3) DESCRIBE, (4) SHOW FIELDS FROM, (5) SHOW COLUMNS FROM, (6) SHOW INDEX FROM, (7) CREATE TABLE, (8) DROP TABLE, (9) ALTER TABLE, (10) DELETE FROM, (11) UPDATE, และ (12) SET PASSWORD
3. CVE-2012-5613 — MySQL (Linux) Database Privilege Elevation Zeroday Exploit
    - ในกรณีที่มีการตั้งค่าระบบให้สิทธิของคำสั่ง FILE แก่ผู้ใช้งานที่ไม่มีสิทธิของผู้ดูแลระบบ ทำให้ผู้ใช้งานดังกล่าวสามารถยกระดับสิทธิของตัวเองโดยการสร้างไฟล์ผ่านคำสั่ง FILE โดยไฟล์ดังกล่าวจะมีสิทธิเทียบเท่ากับไฟล์ที่สร้างโดย MySQL administrator อย่างไรก็ตาม ผู้พัฒนาได้ชี้แจงว่าช่องโหว่ดังกล่าวนี้เกิดจากความผิดพลาดของผู้ดูแลระบบ ที่ไม่ปฏิบัติตามคำแนะนำวิธีการที่ถูกต้องในการติดตั้งระบบ ซึ่งอาจพิจารณานำช่องโหว่ดังกล่าวนี้ออกจากรายการ CVE ในภายหลัง
4. CVE-2012-5614 — MySQL Denial of Service Zeroday PoC
    - ผู้ใช้ที่ได้รับสิทธิในการเข้าถึงระบบสามารถทำ Denial of Service (Mysqld crash) โดยการใช้คำสั่ง SELECT คู่กับคำสั่ง UpdateXML ที่มีข้อมูล XML ประกอบด้วย element ประเภท unique และ nested จำนวนมาก
5. CVE-2012-5615 — MySQL Remote Preauth User Enumeration Zeroday
    - สร้าง Error message โดยใช้ Time delay ตาม Username ที่มีอยู่ในระบบ ซึ่งทำให้ผู้ไม่หวังดีสามารถรู้รายชื่อ Username ที่มีอยู่ในระบบได้

ทั้ง 5 ช่องโหว่นี้มี Proof of Concept Code เผยแพร่ออกสู่สาธารณะแล้ว

## ผลกระทบ

ระบบที่ใช้งาน MySQL เวอร์ชันที่มีช่องโหว่ดังกล่าวอาจถูกผู้ไม่หวังดีเข้าถึงข้อมูลสำคัญ เปลี่ยนแปลงข้อมูลในฐานข้อมูล หรืออาจถูกโจมตีจนระบบไม่สามารถให้บริการต่อได้ (Denial of Service)

## ระบบที่ได้รับผลกระทบ

1. CVE-2012-5611
    - MySQL 5.5.19, 5.1.53 และอาจจะมีในเวอร์ชันอื่นด้วย
    - MariaDB 5.5.2.x ก่อน 5.5.28a, 5.3.x ก่อน 5.3.11, 5.2.x ก่อน 5.2.13 และ 5.1.x ก่อน 5.1.66
2. CVE-2012-5612
    - MySQL 5.5.19 และอาจจะมีในเวอร์ชันอื่นด้วย
    - MariaDB 5.5.28a และอาจจะมีในเวอร์ชันอื่นด้วย
3. CVE-2012-5613
    - MySQL 5.5.19 และอาจจะมีในเวอร์ชันอื่นด้วย
    - MariaDB 5.5.28a และอาจจะมีในเวอร์ชันอื่นด้วย
4. CVE-2012-5614
    - MySQL 5.5.19 และอาจจะมีในเวอร์ชันอื่นด้วย
    - MariaDB 5.5.28a และอาจจะมีในเวอร์ชันอื่นด้วย
5. CVE-2012-5615
    - MySQL 5.5.19 และอาจจะมีในเวอร์ชันอื่นด้วย
    - MariaDB 5.5.28a, 5.3.11, 5.2.13, 5.1.66 และอาจจะมีในเวอร์ชันอื่นด้วย

## ข้อแนะนำในการป้องกันและแก้ไข

ทีมพัฒนาของ MariaDB ซึ่งเป็น MySQL เวอร์ชันที่แยกไปพัฒนาต่อ (Fork) โดยนักพัฒนาภายนอก ได้แก้ไขช่องโหว่ดังกล่าวนี้ในโปรแกรม MariaDB เวอร์ชันล่าสุดแล้ว ผู้ใช้งาน MariaDB สามารถดาวน์โหลดเวอร์ชัน 5.5.28a, 5.3.11, 5.2.13 และ 5.1.66 ไปติดตั้งได้ [36-2] พร้อมกันนี้ ทาง MariaDB ได้ชี้แจงว่าช่องโหว่ CVE-2012-5631 นั้นไม่ใช่ข้อผิดพลาดของโปรแกรมแต่เป็นข้อผิดพลาดของการตั้งค่าระบบ และได้ให้ข้อมูลเพิ่มเติมว่าช่องโหว่ CVE-2012-5615 นั้นมีการค้นพบมานานกว่า 10 ปีแล้ว

อย่างไรก็ตาม ทาง Oracle ผู้พัฒนาโปรแกรม MySQL ยังไม่มีแถลงการณ์ใดๆ เกี่ยวกับช่องโหว่ดังกล่าว ผู้ใช้งาน MySQL ควรติดตามข่าวสารอย่างต่อเนื่องเพื่อหาวิธีป้องกันและแก้ไขปัญหาต่อไป

## อ้างอิง


[36-1] http://www.zdnet.com/vulnerabilities-threaten-to-crash-mysql-databases-7000008194/

[36-2] http://openquery.com/blog/mariadb-security-updates


# 37. ระวังภัย ช่องโหว่ใน Joomla Content Editor อาจถูกฝังมัลแวร์ในเว็บไซต์

**วันที่ประกาศ:** 14 ธันวาคม 2555
**ปรับปรุงล่าสุด:** 14 ธันวาคม 2555
**เรื่อง:** ระวังภัย ช่องโหว่ใน Joomla Content Editor อาจถูกฝังมัลแวร์ในเว็บไซต์
**ประเภทภัยคุกคาม:** Intrusion, Malicious Code

## ข้อมูลทั่วไป

เมื่อวันที่ 12 ธันวาคม 2555 หน่วยงาน Internet Storm Center (ISC) แจ้งว่าได้รับรายงานเว็บไซต์จำนวนมากถูกเจาะระบบและถูกฝังมัลแวร์ลงในหน้าเว็บไซต์ ซึ่งโดยส่วนใหญ่เว็บไซต์เหล่านั้นใช้ Joomla เป็นเครื่องมือในการจัดการเนื้อหา (CMS) [37-1] พร้อมกันนี้ หน่วยงาน CERT-Bund จากประเทศเยอรมนีได้ยืนยันว่าพบการโจมตีดังกล่าวบนเซิร์ฟเวอร์ที่ใช้งาน Joomla ในประเทศเยอรมนีด้วย

ตัวแทนจากหน่วยงาน CERT-Bund ได้ให้ข้อมูลเพิ่มเติมว่า เว็บไซต์ที่ถูกแฮ็กนั้นถูกใช้เพื่อเผยแพร่ซอฟต์แวร์แอนตี้ไวรัสปลอม โดยโค้ดอันตรายดังกล่าวถูกฝังอยู่ในแท็ก iframe [37-2]

เว็บไซต์ Joomla-Downloads ประเทศเยอรมนีได้ชี้แจงว่า หลายๆ เว็บไซต์นั้นถูกแฮ็กโดยใช้สคริปต์ที่เรียกว่า “Bot/0.1 (Bot for JCE)” ที่โจมตีผ่านช่องโหว่ของ Joomla Content Editor ซึ่งสคริปต์ดังกล่าวจะใส่ไฟล์ .gif เข้ามาเซิร์ฟเวอร์ จากนั้นเปลี่ยนชื่อไฟล์ดังกล่าวเป็น story.php ซึ่งเป็น PHP Shell เพื่อใช้ในการแทรกโค้ด iframe ลงในไฟล์ JavaScript สองไฟล์คือ /media/system/js/mootools.js หรือ /media/system/js/caption.js [37-3]

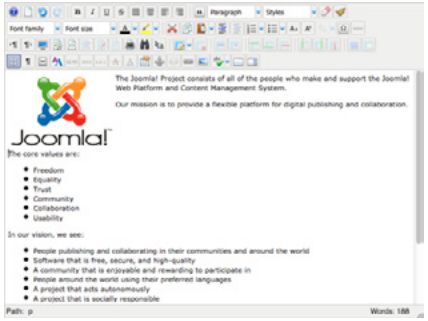
## ผลกระทบ

เว็บไซต์ที่ถูกแฮ็กอาจถูกแทรกโค้ดอันตรายในแท็ก iframe เพื่อ

เผยแพร่มัลแวร์ หรืออาจถูกผู้ไม่หวังดีควบคุมเพื่อใช้ในทางที่ไม่เหมาะสมได้

## ระบบที่ได้รับผลกระทบ

เว็บไซต์ที่ใช้งาน Joomla ที่มีคอมโพเนนต์ Joomla Content Editor เวอร์ชันเก่ากว่า 2.0.11 ตัวอย่างหน้าจอ Joomla Content Editor เป็นดังรูปที่ 38 (37-1)



*รูปที่ 38.รูปที่ 38 (37-1) หน้าจอ Joomla Content Editor [37-4]*

## ข้อแนะนำในการป้องกันและแก้ไข

ผู้ดูแลเว็บไซต์ที่ใช้งาน Joomla ควรตรวจสอบว่าได้มีการติดตั้ง Joomla Content Editor อยู่ในระบบหรือไม่ หากติดตั้งอยู่ควรอัพเดทเป็นเวอร์ชันล่าสุด [37-4] หากพบว่ากำลังใช้งาน JCE เวอร์ชันเก่ากว่า 2.0.11 อยู่ ควรตรวจสอบไฟล์ JavaScipt ว่าถูกฝัง iframe หรือไม่ และควรตรวจสอบไฟล์ PHP Backdoor ซึ่งจะอยู่ที่ /images/stories/story.php หากพบไฟล์ดังกล่าวควรลบออกจากระบบโดยเร็ว

## อ้างอิง


[37-1] https://isc.sans.edu/diary/Joomla+and+WordPress+Bulk+Exploit+Going+on/14677

[37-2] http://www.h-online.com/security/news/item/Joomla-sites-misused-to-deploy-malware-1766841.html

[37-3] http://www.joomla-downloads.de/blick-ueberden-tellerrand/1998-alte-versionen-des-jce-sind-ziel-von-massenhacks.html

[37-4] http://www.joomlacontenteditor.net/


# 38. ระวังภัย ช่องโหว่ใน Samsung Galaxy (S2, S3, Note, Note2) สามารถ root หรือทำเครื่อง Brick ได้

**วันที่ประกาศ:** 17 ธันวาคม 2555
**ปรับปรุงล่าสุด:** 17 ธันวาคม 2555
**เรื่อง:** ระวังภัย ช่องโหว่ใน Samsung Galaxy (S2, S3, Note, Note2) สามารถ root หรือทำเครื่อง Brick ได้
**ประเภทภัยคุกคาม:** Intrusion, Malicious Code

## ข้อมูลทั่วไป

นักพัฒนาชื่อ alephzain ได้โพสต์ใน Forum ของเว็บไซต์ xda-developers ว่าได้ค้นพบช่องโหว่ใน Kernel ของโทรศัพท์มือถือ Samsung Galaxy S3 และโทรศัพท์มือถือเครื่องอื่นๆ ที่ใช้ชิป Exynos ของ Samsung สาเหตุของช่องโหว่ดังกล่าวเกิดจากไฟล์ /dev/exynos-mem นั้นถูกตั้งค่า Permission เป็น R/W ทำให้ผู้ใช้หรือแอปพลิเคชันใดๆ ก็ตามสามารถเข้าถึงหน่วยความจำได้โดยตรง (Direct memory access) ผ่านไฟล์ดังกล่าว หรือผ่านไลบรารีที่เรียกใช้งานไฟล์ดังกล่าว ซึ่งประกอบด้วย 3 ไฟล์คือ

- /system/lib/hw/camera.smdk4x12.so
- /system/lib/hw/gralloc.smdk4x12.so
- /system/lib/libhdmi.so

ซึ่งไฟล์ไลบรารีดังกล่าว ใช้สำหรับการควบคุมกล้อง ควบคุมการแสดงผลด้านกราฟฟิก หรือใช้สำหรับแสดงผลผ่านพอร์ต HDMI ซึ่งนักพัฒนาพบว่าแอปพลิเคชันของ Samsung นั้นมีการเรียกใช้ไฟล์ไลบรารีดังกล่าว [38-1]

นักพัฒนาชื่อ Chainfire ได้สร้างแอปพลิเคชันเพื่อทดสอบการโจมตีผ่านช่องโหว่ดังกล่าว โดยแอปพลิเคชันที่พัฒนานั้นชื่อว่า ExynosAbuse เมื่อสั่งให้ทำงาน แอปพลิเคชันดังกล่าวจะได้สิทธิของ root และติดตั้งโปรแกรม SuperSU เพื่อใช้มอบสิทธิของ root ให้กับแอปพลิเคชันอื่นต่อไป

## ผลกระทบ

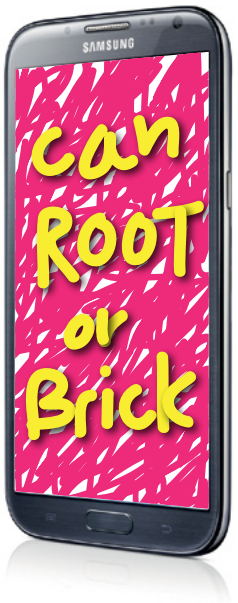
ผู้ไม่หวังดีสามารถสร้างแอปพลิเคชันที่สามารถเข้าถึงข้อมูลของผู้ใช้ ลบข้อมูลทั้งหมดในเครื่อง หรือทำให้เครื่อง Brick ได้ [38-2]

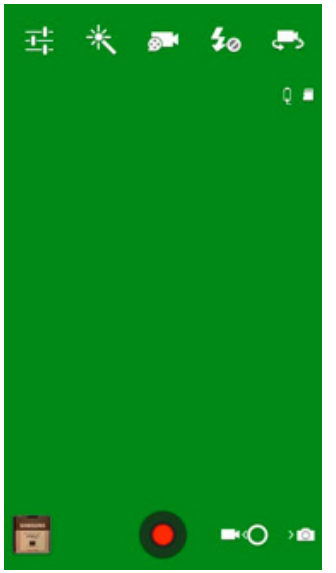
## ระบบที่ได้รับผลกระทบ

- Samsung Galaxy S2 GT-I9100
- Samsung Galaxy S3 GT-I9300
- Samsung Galaxy S3 LTE GT-I9305
- Samsung Galaxy Note GT-N7000
- Samsung Galaxy Note 2 GT-N7100
- Verizon Galaxy Note 2 SCH-I605 (with locked bootloaders)
- Samsung Galaxy Note 10.1 GT-N8000
- Samsung Galaxy Note 10.1 GT-N8010

## ข้อแนะนำในการป้องกันและแก้ไข

นักพัฒนาพบว่า การแก้ไขค่า Permission ของไฟล์ที่เกี่ยวข้องกับ Kernel สามารถป้องกันปัญหาดังกล่าวได้ โดยแอปพลิเคชัน ExynosAbuse เวอร์ชัน 1.10 นั้นนอกจากจะใช้ root เครื่องได้แล้วยังสามารถแก้ไข Permission ของไฟล์เพื่อปิดช่องโหว่ดังกล่าวได้ อย่างไรก็ตาม การกระทำดังกล่าวส่งผลต่อการใช้งานแอปพลิเคชันของ Samsung เช่น กล้องถ่ายรูปจะไม่สามารถใช้งานได้ [38-3] ดังรูปที่ 39 (38-1) อย่างไรก็ตามผู้ใช้ยังสามารถสลับให้เปิดช่องโหว่ไว้เพื่อใช้งานกล้องได้



*รูปที่ 39.รูปที่ 39 (38-1) กล้องถ่ายรูปไม่สามารถใช้งานได้หลังการแก้ไข Permission ของไฟล์*

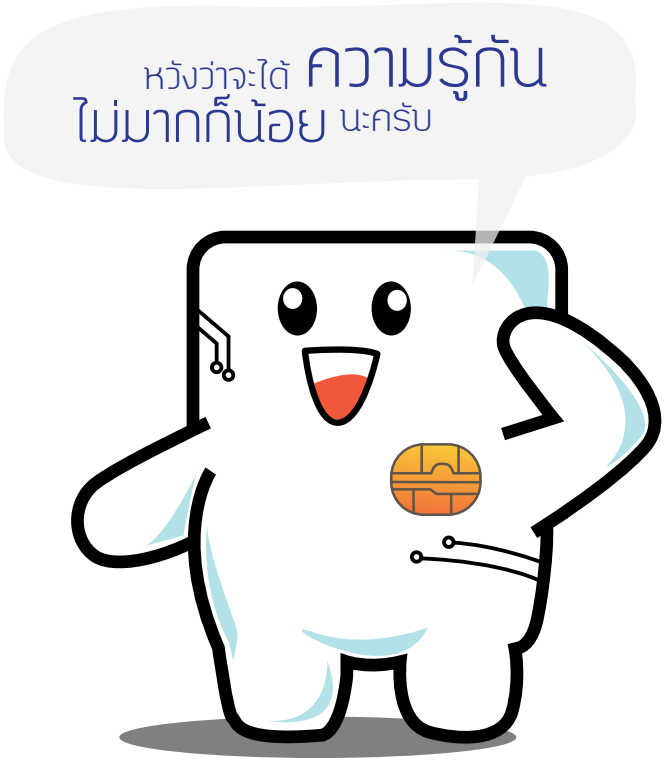
นักพัฒนาได้แจ้งช่องโหว่ดังกล่าวนี้ให้ทาง Samsung ทราบแล้ว แต่ในขณะนี้ยังไม่มีประกาศอย่างเป็นทางการจาก Samsung ผู้ใช้งานโทรศัพท์มือถือที่ได้รับผลกระทบจากช่องโหว่ดังกล่าว ไม่ควรติดตั้ง แอปพลิเคชันที่ไม่น่าเชื่อถือ รวมทั้งติดตามข่าวสารและการอัพเดทระบบปฏิบัติการอยู่เสมอ

## อ้างอิง


[38-1] http://forum.xda-developers.com/showthread.php?p=35469999

[38-2] http://thenextweb.com/mobile/2012/12/16/new-exploit-could-give-android-malware-apps-access-to-user-data-on-samsung-gs-iii-other-devices/

[38-3] http://forum.xda-developers.com/showthread.php?t=2050297


หวังว่าจะได้ ความรู้กัน
ไม่มากก็น้อย นะครับ

จัดพิมพ์และเผยแพร่โดย
**ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)**

**สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)**
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 เลขที่ 120 หมู่ 3อาคารรัฐประศาสนภักดี
(อาคาร B) ชั้น 7 ถ.แจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

เว็บไซต์ไทยเซิร์ต www.thaicert.or.th
เว็บไซต์สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) www.etda.or.th
เว็บไซต์กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร www.mict.go.th

ISBN : 978-974-9765-43-2