

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

Product Focus

[Apache Chunked Vulnerability Scanner](#) - The S4 Apache Chunked Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Apache Chunked Encoding buffer overflow.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

The Sony data breach more widespread. Warning about fake video with virus. Password manager users urged to change password after possible breach. DOS possible on IPV6.

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.

(503) 524 5758 or sales@netvigilance.com

Top Security News Stories this Week

• Sony says PlayStation breach extended to other systems

Investigation into the breach of Sony's PlayStation Network and Qriocity services has turned up further compromise, the company disclosed Monday.

Sony said it temporarily has disconnected its online gaming portal, known as Sony Online Entertainment (SOE), after discovering that the personal information connected to an unknown number of users' accounts may have been stolen. The data includes names, street addresses, email addresses, genders, birth dates, telephone numbers, login names and hashed passwords.

In addition, the hackers likely got their hands on 23,400 credit and debit card numbers belonging to SOE customers in Germany, Austria, the Netherlands and Spain. SC Magazine

Full Story :

http://www.scmagazineus.com/sony-says-playstation-breach-extended-to-other-systems/article/201992/?utm_source

• FBI warns that fake bin Laden video is a virus

IDG News Service - The U.S. Federal Bureau of Investigation warned computer users Tuesday that messages claiming to include photos and videos of Osama bin Laden's death actually contain a virus that could steal personal information.

The warning comes as security companies said that they've spotted the first samples of malicious software disguised as photos of the dead Al Qaeda leader.

Security vendor F-Secure said Tuesday that criminals are e-mailing a password-stealing Trojan horse program called Banload to victims, and Symantec said it's seen criminals spamming victims with links to fake "Osama dead" news articles that launch Web-based attacks on visitors. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9216389/FBI warns that fake bin Laden video is a virus?source=rss_se](http://www.computerworld.com/s/article/9216389/FBI_warns_that_fake_bin_Laden_video_is_a_virus?source=rss_se)

• LastPass forcing members to change passwords

Users who manage and store their passwords through password management service LastPass are being forced to change their master passwords after the site noticed an issue this week that raised the spectre of a possible security breach.

As described in a blog yesterday, LastPass (download) recently followed a string of breadcrumbs that pointed to an anomaly in its network traffic on Tuesday. Though such anomalies aren't unusual, LastPass found a matching anomaly in one of its databases. Unable to identify a root cause for either anomaly, the company made the decision to assume the worst--that some of its data had been hacked.

Although LastPass hasn't identified a specific breach, it's erring on the side of caution by now forcing its members to change their master passwords. For you non-LastPass users, what exactly does that mean? Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20060004-83.html?part=rss&subj=news&tag=2547-1_3-0-20

• Microsoft, Juniper urged to patch dangerous IPv6 DoS hole

Network World - Security experts are urging Microsoft and Juniper to patch a year-old IPv6 vulnerability so dangerous it can freeze any Windows machine on a LAN in a matter of minutes.

Microsoft has downplayed the risk because the hole requires a physical connection to the wired LAN. Juniper says it has delayed a patch because the hole only affects a small number of its products and it wants the IETF to fix the protocol instead.

SEE IT YOURSELF: How to use a known IPv6 hole to fast-freeze a Windows network Computerworld

Full Story :

[http://www.computerworld.com/s/article/9216396/Microsoft Juniper urged to patch dangerous IPv6 DoS hole?so](http://www.computerworld.com/s/article/9216396/Microsoft_Juniper_urged_to_patch_dangerous_IPv6_DoS_hole?so)

New Vulnerabilities Tested in SecureScout

• 19284 Win32k Use After Free Vulnerability (CVE-2011-0672) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47207

<http://www.securityfocus.com/bid/47207>

* OSVDB: 71746

<http://osvdb.org/71746>

* SECTRACK: 1025345
<http://www.securitytracker.com/id?1025345>
* SECUNIA: 44156
<http://secunia.com/advisories/44156>
* VUPEN: ADV-2011-0952
<http://www.vupen.com/english/advisories/2011/0952>
* XF: mswin-win32k-var7-priv-escalation(66401)
<http://xforce.iss.net/xforce/xfdb/66401>

CVE Reference:

CVE-2011-0672 (cve.mitre.org, nvd.nist.gov)

• **19285 Win32k Use After Free Vulnerability (CVE-2011-0674) (MS11-034/2506223) (Remote File Checking)**

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MISC:
<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>
* CONFIRM:
<http://support.avaya.com/css/P8/documents/100133352>
* MS: MS11-034
<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>
* BID: 47209
<http://www.securityfocus.com/bid/47209>
* OSVDB: 71747
<http://osvdb.org/71747>
* SECTRACK: 1025345
<http://www.securitytracker.com/id?1025345>
* SECUNIA: 44156
<http://secunia.com/advisories/44156>
* VUPEN: ADV-2011-0952
<http://www.vupen.com/english/advisories/2011/0952>
* XF: mswin-win32k-var9-priv-escalation(66403)
<http://xforce.iss.net/xforce/xfdb/66403>

CVE Reference:

CVE-2011-0674 (cve.mitre.org, nvd.nist.gov)

• **19286 Win32k Use After Free Vulnerability (CVE-2011-0675) (MS11-034/2506223) (Remote File Checking)**

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MISC:
<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>
* CONFIRM:
<http://support.avaya.com/css/P8/documents/100133352>
* MS: MS11-034
<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>
* BID: 47210
<http://www.securityfocus.com/bid/47210>
* OSVDB: 71748
<http://osvdb.org/71748>
* SECTRACK: 1025345
<http://www.securitytracker.com/id?1025345>
* SECUNIA: 44156
<http://secunia.com/advisories/44156>
* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var10-priv-escalation(66404)

<http://xforce.iss.net/xforce/xfdb/66404>

CVE Reference:

CVE-2011-0675 (cve.mitre.org, nvd.nist.gov)

• 19287 Win32k Use After Free Vulnerability (CVE-2011-1234) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47211

<http://www.securityfocus.com/bid/47211>

* OSVDB: 71749

<http://osvdb.org/71749>

* SECTRACK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var22-priv-escalation(66416)

<http://xforce.iss.net/xforce/xfdb/66416>

CVE Reference:

CVE-2011-1234 (cve.mitre.org, nvd.nist.gov)

• 19314 Win32k Use After Free Vulnerability (CVE-2011-1235) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47212

<http://www.securityfocus.com/bid/47212>

* OSVDB: 71750

<http://osvdb.org/71750>

* SECTRACK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var23-priv-escalation(66417)

<http://xforce.iss.net/xforce/xfdb/66417>

CVE Reference:

CVE-2011-1235 (cve.mitre.org, nvd.nist.gov)

• **19315 Win32k Use After Free Vulnerability (CVE-2011-1236) (MS11-034/2506223) (Remote File Checking)**

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47213

<http://www.securityfocus.com/bid/47213>

* OSVDB: 71751

<http://osvdb.org/71751>

* SECTRAK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var24-priv-escalation(66418)

<http://xforce.iss.net/xforce/xfdb/66418>

CVE Reference:

CVE-2011-1236 (cve.mitre.org, nvd.nist.gov)

• **19316 Win32k Use After Free Vulnerability (CVE-2011-1237) (MS11-034/2506223) (Remote File Checking)**

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47214

<http://www.securityfocus.com/bid/47214>

* OSVDB: 71752

<http://osvdb.org/71752>

* SECTRAK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var25-priv-escalation(66419)

<http://xforce.iss.net/xforce/xfdb/66419>

CVE Reference:

CVE-2011-1237 (cve.mitre.org, nvd.nist.gov)

• **19317 Win32k Use After Free Vulnerability (CVE-2011-1238) (MS11-034/2506223) (Remote File Checking)**

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47215

<http://www.securityfocus.com/bid/47215>

* OSVDB: 71753

<http://osvdb.org/71753>

* SECTRACK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var26-priv-escalation(66420)

<http://xforce.iss.net/xforce/xfdb/66420>

CVE Reference:

CVE-2011-1238 (cve.mitre.org, nvd.nist.gov)

• 19318 Win32k Use After Free Vulnerability (CVE-2011-1239) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47216

<http://www.securityfocus.com/bid/47216>

* OSVDB: 71754

<http://osvdb.org/71754>

* SECTRACK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var27-priv-escalation(66421)

<http://xforce.iss.net/xforce/xfdb/66421>

CVE Reference:

CVE-2011-1239 (cve.mitre.org, nvd.nist.gov)

• 19319 Win32k Use After Free Vulnerability (CVE-2011-1240) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

- * MISC:
<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>
- * CONFIRM:
<http://support.avaya.com/css/P8/documents/100133352>
- * MS: MS11-034
<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>
- * BID: 47217
<http://www.securityfocus.com/bid/47217>
- * OSVDB: 71755
<http://osvdb.org/71755>
- * SECTRAK: 1025345
<http://www.securitytracker.com/id?1025345>
- * SECUNIA: 44156
<http://secunia.com/advisories/44156>
- * VUPEN: ADV-2011-0952
<http://www.vupen.com/english/advisories/2011/0952>
- * XF: mswin-win32k-var28-priv-escalation(66422)
<http://xforce.iss.net/xforce/xfdb/66422>

CVE Reference:

CVE-2011-1240 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-1845 Microsoft CVSS 2.0 Score = 7.8

Multiple memory leaks in the DataGrid control implementation in Microsoft Silverlight 4 before 4.0.60310.0 allow remote attackers to cause a denial of service (memory consumption) via an application involving (1) subscriptions to an INotifyDataErrorInfo.ErrorsChanged event or (2) a TextBlock or TextBox element.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

- MSKB: <http://support.microsoft.com/kb/2526954>
- MISC: <http://isc.sans.edu/diary.html?storyid=10747>

CVE Reference: [CVE-2011-1845](http://cve.mitre.org/cve/2011/1845)

• CVE-2011-1844 Microsoft CVSS 2.0 Score = 7.8

Memory leak in Microsoft Silverlight 4 before 4.0.60310.0 allows remote attackers to cause a denial of service (memory consumption) via an application involving a popup control and a custom DependencyProperty property, related to lack of garbage collection.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

- MSKB: <http://support.microsoft.com/kb/2526954>
- MISC: <http://isc.sans.edu/diary.html?storyid=10747>

CVE Reference: [CVE-2011-1844](http://cve.mitre.org/cve/2011/1844)

• CVE-2011-1545 HP CVSS 2.0 Score = 6.8

Cross-site request forgery (CSRF) vulnerability in HP Insight Control Performance Management before 6.3 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

- HP: <http://marc.info/?l=bugtraq&m=130339248106264&w=2>
- HP: <http://marc.info/?l=bugtraq&m=130339248106264&w=2>

CVE Reference: [CVE-2011-1545](http://cve.mitre.org/cve/2011/1545)

• **CVE-2011-1544 HP CVSS 2.0 Score = 6.0**

Unspecified vulnerability in HP Insight Control Performance Management before 6.3 allows remote authenticated users to gain privileges via unknown vectors.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

HP: <http://marc.info/?l=bugtraq&m=130339248106264&w=2>

HP: <http://marc.info/?l=bugtraq&m=130339248106264&w=2>

CVE Reference: [CVE-2011-1544](#)

• **CVE-2011-1724 HP CVSS 2.0 Score = 6.0**

Unspecified vulnerability in HP Virtual Server Environment before 6.3 allows remote authenticated users to gain privileges via unknown vectors.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

HP: <http://marc.info/?l=bugtraq&m=130339296506866&w=2>

HP: <http://marc.info/?l=bugtraq&m=130339296506866&w=2>

CVE Reference: [CVE-2011-1724](#)

• **CVE-2011-1539 HP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in HP Proliant Support Pack (PSP) before 8.7 allows remote attackers to obtain sensitive information via unknown vectors.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

HP: <http://marc.info/?l=bugtraq&m=130331221326039&w=2>

HP: <http://marc.info/?l=bugtraq&m=130331221326039&w=2>

CVE Reference: [CVE-2011-1539](#)

• **CVE-2011-1538 HP CVSS 2.0 Score = 4.9**

Open redirect vulnerability in HP Proliant Support Pack (PSP) before 8.7 allows remote authenticated users to redirect other users to arbitrary web sites and conduct phishing attacks via unspecified vectors.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

HP: <http://marc.info/?l=bugtraq&m=130331221326039&w=2>

HP: <http://marc.info/?l=bugtraq&m=130331221326039&w=2>

CVE Reference: [CVE-2011-1538](#)

• **CVE-2011-1537 HP CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in HP Proliant Support Pack (PSP) before 8.7 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

HP: <http://marc.info/?l=bugtraq&m=130331221326039&w=2>

HP: <http://marc.info/?l=bugtraq&m=130331221326039&w=2>

CVE Reference: [CVE-2011-1537](#)

Vulnerability Resource

Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. <http://www.infosyssec.org/infosyssec/>

Thank You

Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com

About SecureScout

SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.

SecureScout is a trademark of NexantiS Corporation.

netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:

Customers in America and Northern Europe contact us at info@netVigilance.com

Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net