

2011 Issue #16

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

Applications aren't secure enough. Laboratory had to shut down after attack. Critical infrastructure companies under attack. Security not a priority.

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

• New report finds most applications don't pass security tests

A new report issued on Tuesday by security firm Veracode paints a grim picture of the amount of protection built into application software.

More than half of all applications fail to meet acceptable security quality, according to the "State of Software Security Report: The Intractable Problem of Insecure Software."

The study, which assessed nearly 5,000 applications over the last 18 months, found that 58 percent of all applications had "unacceptable" security quality when initially submitted to Veracode's testing platform. Further, more than eight out of 10 web applications failed when measured against the OWASP Top 10, an industry benchmark that documents the most common critical web application errors. SC Magazine

Full Story :

http://www.scmagazineus.com/new-report-finds-most-applications-dont-pass-security-tests/article/201029/?utm_source

• Oak Ridge National Lab shuts down Internet, email after cyberattack

Computerworld - The Oak Ridge National Laboratory, home to one of the world's most powerful supercomputers, has been forced to shut down its email systems and all Internet access for employees since late last Friday, following a sophisticated cyberattack.

The restrictions on Internet access will remain in place until those investigating the attack know for sure that it has been completely contained, said Barbara Penland, ORNL's director of communications.

The lab is expected to restore external email service sometime on Wednesday, however no attachments will be allowed for the time being. Computerworld

Full Story :

http://www.computerworld.com/s/article/9215962/Oak_Ridge_National_Lab_shuts_down_Internet_email_after_cyber

• Cyber attacks rise at critical infrastructure firms

Cyber attacks are on the rise in critical infrastructure companies, a new report shows.

(Credit: CSIS/McAfee)

Cyber attacks on critical infrastructure companies are on the rise, with a jump in extortion attempts and malware designed to sabotage systems, like Stuxnet, according to a new report. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20055091-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Despite threats, security not enough of priority at utilities

Critical infrastructure providers have been slow to respond to an increasing number of threats targeting industries such as power, oil, gas and water, according to a new report.

According to a joint study from McAfee and the Center for Strategic and International Studies (CSIS), which surveyed 200 IT security executives working at utilities in 14 countries, 40 percent believe their sector's vulnerability to attack has increased since last year.

The stats agree. Last year's version of the study found that roughly half of the respondents never faced a major denial-of-service attack or network intrusion. But this year, that number rose to 80 and 85 percent, respectively. SC Magazine

Full Story :

http://www.scmagazineus.com/despite-threats-security-not-enough-of-priority-at-utilities/article/201046/?utm_source

• 8 security questions to ask before building mobile apps

CSO - Enterprise organizations are rushing to build iPhone, iPad, Android and BlackBerry applications to deepen their customer experiences and extend the ways their customers can purchase from them.

The demand for these applications is driving development at a rapid pace. Unfortunately, the risks associated with mobile applications are different from typical enterprise software. Also, security is rarely a project driver in the mobile software world.

[Also see: Malware exploding, especially on mobile devices] Computerworld

Full Story :

http://www.computerworld.com/s/article/9215912/8_security_questions_to_ask_before_building_mobile_apps?source

New Vulnerabilities Tested in SecureScout

• 19264 Excel Integer Overrun Vulnerability (MS11-021/2489279) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. 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** Risk: **High**

References:

* MISC:

http://secunia.com/secunia_research/2011-31

* MS: MS11-021
<http://www.microsoft.com/technet/security/Bulletin/MS11-021.msp>
* BID: 47201
<http://www.securityfocus.com/bid/47201>
* OSVDB: 71758
<http://osvdb.org/71758>
* SECTRACK: 1025337
<http://www.securitytracker.com/id?1025337>
* SECUNIA: 39122
<http://secunia.com/advisories/39122>
* VUPEN: ADV-2011-0940
<http://www.vupen.com/english/advisories/2011/0940>

CVE Reference:

CVE-2011-0097 (cve.mitre.org, nvd.nist.gov)

● **19265 Excel Heap Overflow Vulnerability (MS11-021/2489279) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. 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** Risk: **High**

References:

* MISC:
http://secunia.com/secunia_research/2011-32/
* MS: MS11-021
<http://www.microsoft.com/technet/security/Bulletin/MS11-021.msp>
* BID: 47235
<http://www.securityfocus.com/bid/47235>
* OSVDB: 71759
<http://osvdb.org/71759>
* SECTRACK: 1025337
<http://www.securitytracker.com/id?1025337>
* SECUNIA: 39122
<http://secunia.com/advisories/39122>
* VUPEN: ADV-2011-0940
<http://www.vupen.com/english/advisories/2011/0940>

CVE Reference:

CVE-2011-0098 (cve.mitre.org, nvd.nist.gov)

● **19266 Excel Record Parsing WriteAV Vulnerability (MS11-021/2489279) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. 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** Risk: **High**

References:

* BUGTRAQ: 20110412 ZDI-11-120: Microsoft Office Excel RealTimeData Record Parsing Remote Code Execution Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/517463/100/0/threaded>
* MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-11-120>
* MS: MS11-021
<http://www.microsoft.com/technet/security/Bulletin/MS11-021.msp>
* BID: 47243
<http://www.securityfocus.com/bid/47243>
* OSVDB: 71766
<http://osvdb.org/71766>
* SECTRACK: 1025337
<http://www.securitytracker.com/id?1025337>
* SECUNIA: 39122
<http://secunia.com/advisories/39122>
* VUPEN: ADV-2011-0940
<http://www.vupen.com/english/advisories/2011/0940>

CVE Reference:

CVE-2011-0101 (cve.mitre.org, nvd.nist.gov)

• 19267 Excel Memory Corruption Vulnerability (MS11-021/2489279) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. 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** Risk: **High**

References:

* IDEFENSE: 20110412 Microsoft Excel Memory Corruption Vulnerability

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=901>

* MS: MS11-021

<http://www.microsoft.com/technet/security/Bulletin/MS11-021.mspx>

* BID: 47244

<http://www.securityfocus.com/bid/47244>

* OSVDB: 71760

<http://osvdb.org/71760>

* SECTRAK: 1025337

<http://www.securitytracker.com/id?1025337>

* SECUNIA: 39122

<http://secunia.com/advisories/39122>

* VUPEN: ADV-2011-0940

<http://www.vupen.com/english/advisories/2011/0940>

CVE Reference:

CVE-2011-0103 (cve.mitre.org, nvd.nist.gov)

• 19268 Excel Buffer Overwrite Vulnerability (MS11-021/2489279) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. 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** Risk: **High**

References:

* MISC:

<http://www.checkpoint.com/defense/advisories/public/2011/cpai-31-Mard.html>

* MS: MS11-021

<http://www.microsoft.com/technet/security/Bulletin/MS11-021.mspx>

* BID: 47245

<http://www.securityfocus.com/bid/47245>

* OSVDB: 71761

<http://osvdb.org/71761>

* SECTRAK: 1025337

<http://www.securitytracker.com/id?1025337>

* SECUNIA: 39122

<http://secunia.com/advisories/39122>

* VUPEN: ADV-2011-0940

<http://www.vupen.com/english/advisories/2011/0940>

CVE Reference:

CVE-2011-0104 (cve.mitre.org, nvd.nist.gov)

• 19269 Excel Data Initialization Vulnerability (MS11-021/2489279) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. 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** Risk: **High**

References:

* MS: MS11-021

<http://www.microsoft.com/technet/security/Bulletin/MS11-021.mspx>

* SECTRAK: 1025337

<http://www.securitytracker.com/id?1025337>

* SECUNIA: 39122

<http://secunia.com/advisories/39122>

* VUPEN: ADV-2011-0940

<http://www.vupen.com/english/advisories/2011/0940>

* BID: 47256

<http://www.securityfocus.com/bid/47256>

CVE Reference:

CVE-2011-0105 (cve.mitre.org, nvd.nist.gov)

• 19270 Excel Array Indexing Vulnerability (MS11-021/2489279) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. 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** Risk: **High**

References:

* MISC:

<http://dvlabs.tippingpoint.com/blog/2011/02/07/zdi-disclosure-microsoft>

* MISC:

<http://zerodayinitiative.com/advisories/ZDI-11-042/>

* MS: MS11-021

<http://www.microsoft.com/technet/security/Bulletin/MS11-021.msp>

* SECTRACK: 1025337

<http://www.securitytracker.com/id?1025337>

* SECUNIA: 43232

<http://secunia.com/advisories/43232>

* SECUNIA: 39122

<http://secunia.com/advisories/39122>

* VUPEN: ADV-2011-0940

<http://www.vupen.com/english/advisories/2011/0940>

CVE Reference:

CVE-2011-0978 (cve.mitre.org, nvd.nist.gov)

• 19271 Excel Linked List Corruption Vulnerability (MS11-021/2489279) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. 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** Risk: **High**

References:

* MISC:

<http://dvlabs.tippingpoint.com/blog/2011/02/07/zdi-disclosure-microsoft>

* MISC:

<http://zerodayinitiative.com/advisories/ZDI-11-041/>

* MS: MS11-021

<http://www.microsoft.com/technet/security/Bulletin/MS11-021.msp>

* OSVDB: 70904

<http://osvdb.org/70904>

* SECTRACK: 1025337

<http://www.securitytracker.com/id?1025337>

* SECUNIA: 43231

<http://secunia.com/advisories/43231>

* SECUNIA: 39122

<http://secunia.com/advisories/39122>

* VUPEN: ADV-2011-0940

<http://www.vupen.com/english/advisories/2011/0940>

CVE Reference:

CVE-2011-0979 (cve.mitre.org, nvd.nist.gov)

• 19272 Excel Dangling Pointer Vulnerability (MS11-021/2489279) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. 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** Risk: **High**

References:

- * MISC:
<http://dvlabs.tippingpoint.com/blog/2011/02/07/zdi-disclosure-microsoft>
- * MISC:
<http://zerodayinitiative.com/advisories/ZDI-11-040/>
- * MS: MS11-021
<http://www.microsoft.com/technet/security/Bulletin/MS11-021.msp>
- * SECTRACK: 1025337
<http://www.securitytracker.com/id?1025337>
- * SECUNIA: 43210
<http://secunia.com/advisories/43210>
- * SECUNIA: 39122
<http://secunia.com/advisories/39122>
- * VUPEN: ADV-2011-0940
<http://www.vupen.com/english/advisories/2011/0940>

CVE Reference:

CVE-2011-0980 (cve.mitre.org, nvd.nist.gov)

• 19273 Floating Point Techno-color Time Bandit RCE Vulnerability (MS11-022/2489283) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

- * MS: MS11-022
<http://www.microsoft.com/technet/security/Bulletin/MS11-022.msp>
- * SECTRACK: 1025340
<http://www.securitytracker.com/id?1025340>
- * VUPEN: ADV-2011-0941
<http://www.vupen.com/english/advisories/2011/0941>
- * BID: 47252
<http://www.securityfocus.com/bid/47252>

CVE Reference:

CVE-2011-0655 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-0807 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in Oracle Sun GlassFish Enterprise Server 2.1, 2.1.1, and 3.0.1, and Sun Java System Application Server 9.1, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Administration.

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

References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

CVE Reference: [CVE-2011-0807](http://cve.mitre.org/cve/2011/0807)

• CVE-2011-0825 Oracle CVSS 2.0 Score = 6.8

Unspecified vulnerability in Oracle JD Edwards EnterpriseOne Tools 8.9 GA through 8.98.4.1 and OneWorld Tools through 24.1.3 allows remote attackers to affect confidentiality, integrity, and availability, related to Enterprise Infrastructure SEC.

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

References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

CVE Reference: [CVE-2011-0825](#)

• **CVE-2011-0799 Oracle CVSS 2.0 Score = 6.5**

Unspecified vulnerability in the Oracle Warehouse Builder component in Oracle Database Server 10.2.0.5 (OWB), 11.1.0.7, and 11.2.0.1 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Oracle Warehouse Builder User Account.

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

References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

CVE Reference: [CVE-2011-0799](#)

• **CVE-2011-0792 Oracle CVSS 2.0 Score = 6.5**

Unspecified vulnerability in the Oracle Warehouse Builder component in Oracle Database Server 10.2.0.5 (OWB) and 11.1.0.7 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Dimensional Data Modeling.

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

References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

CVE Reference: [CVE-2011-0792](#)

• **CVE-2011-0824 Oracle CVSS 2.0 Score = 6.4**

Unspecified vulnerability in Oracle JD Edwards EnterpriseOne Tools 8.9 GA through 8.98.4.1 and OneWorld Tools through 24.1.3 allows remote attackers to affect confidentiality and integrity, related to Enterprise Infrastructure SEC.

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

References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

CVE Reference: [CVE-2011-0824](#)

• **CVE-2011-0803 Oracle CVSS 2.0 Score = 5.8**

Unspecified vulnerability in the JD Edwards EnterpriseOne Tools component in Oracle JD Edwards Products 8.9 GA through 8.98.4.1, and OneWorld Tools through 24.1.3, allows remote attackers to affect integrity and availability, related to Enterprise Infrastructure SEC.

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

References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

CVE Reference: [CVE-2011-0803](#)

• **CVE-2011-0861 Oracle CVSS 2.0 Score = 5.5**

Unspecified vulnerability in Oracle PeopleSoft Enterprise HRMS 9.0 Update 2011-B and 9.1 Update 2011-B allows remote authenticated users to affect confidentiality and integrity via unknown vectors related to Global Payroll Core.

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

References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

CVE Reference: [CVE-2011-0861](#)

• **CVE-2009-5071 HP CVSS 2.0 Score = 10.0**

Unspecified vulnerability in Palm Pre WebOS before 1.2.1 has unknown impact and attack vectors related to an "included contact template file."

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

References:

CONFIRM: http://kb.palm.com/wps/portal/kb/na/pre/p100eww/sprint/solutions/article/50607_en.html#121

CVE Reference: [CVE-2009-5071](https://cve.mitre.org/cve/2009/5071)

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