

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://www2.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

New system to help developers improve on security. New botnet currently impossible to break. Spear phishing gaining popularity. \$2.7 million stolen from Citigroup customers.

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

• DHS unveils new programs for software security

A group of public and private-sector organizations have teamed up to create a new risk analysis framework and scoring system aimed at helping developers and consumers improve the security of their software. The Common Weakness Risk Analysis Framework (CWRAF), released Monday by the U.S. Department of Homeland Security, in conjunction with the SANS Institute and nonprofit government technology research contractor Mitre, offers a way for organizations to evaluate which software weaknesses pose the greatest risk to their organization.

The companion Common Weakness Scoring System (CWSS), also released Monday, is meant to help organizations prioritize unfixed vulnerabilities in their software.

Several security vendors, including Cenzic, Fortify Software and Klocwork, have already announced plans to incorporate the scoring system into their future offerings, Bob Martin, program director of Mitre, told SCMagazineUS.com on Monday. SC Magazine

Full Story :

• **TDL-4: The 'indestructible' botnet?**

Security researchers at Kaspersky Lab have detailed a new botnet--a collection of infected computers controlled by cybercriminals--called TDL-4, that might just be "indestructible."

TDL-4 gets its name by being the fourth generation of the botnet. In 2008, the original TDL appeared. It has been altered over the last several years. With TDL-4, Kaspersky has found, the malware creators have drastically improved the botnet over its predecessors.

"The malware writers extended the program functionality, changed the algorithm used to encrypt the communication protocol between bots and the botnet command and control servers, and attempted to ensure they had access to infected computers even in cases where the botnet control centers are shut down," Kaspersky wrote on its SecureList blog earlier this week. "The owners of TDL are essentially trying to create an 'indestructible' botnet that is protected against attacks, competitors, and antivirus companies." Cnet Security

Full Story :

http://news.cnet.com/8301-13506_3-20075725-17/tdl-4-the-indestructible-botnet/?part=rss&subj=news&tag=2547-1_3

• **Crooks opt for spear phishing despite higher upfront cost**

A report released Thursday by Cisco confirms what may have become fairly obvious to security professionals and industry followers over recent months: Cybercriminals are scrapping widespread malicious email campaigns for more targeted attacks.

"Cybercriminals are balancing competing priorities," the report said. "Infect more users or keep the attack small enough to fly under security vendors' radar."

One side appears to be winning out. The Cisco white paper, "Email Attacks: This Time it's Personal," reveals a dramatic drop in profits accrued by crooks who launch traditional attacks, such as delivering malware-laden or phishing emails. SC Magazine

Full Story :

http://www.scmagazineus.com/crooks-opt-for-spear-phishing-despite-higher-upfront-cost/article/206586/?utm_source

• **Citigroup hacking nets \$2.7 million from customers**

About 3,400 Citigroup credit card customers suffered a loss of \$2.7 million during a security breach earlier this year, according to a Wall Street Journal report.

Citi acknowledged earlier this month that a May 10 breach compromised the company's online account system, allowing the attackers to access names, account numbers, and contact information for the affected customers. However, Citi said that Social Security numbers, birth dates, card expiration dates, and card security codes were not compromised.

The banking giant said its customers will not be liable for the losses. Cnet Security

Full Story :

[http://news.cnet.com/8301-1009_3-20074570-83/citigroup-hacking-nets-\\$2.7-million-from-customers/?part=rss&subj](http://news.cnet.com/8301-1009_3-20074570-83/citigroup-hacking-nets-$2.7-million-from-customers/?part=rss&subj)

New Vulnerabilities Tested in SecureScout

• **19381 Excel Insufficient Record Validation Vulnerability (MS11-045/2537146) (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: MS11-045

<http://www.microsoft.com/technet/security/Bulletin/MS11-045.mspx>

* BID: 48157

<http://www.securityfocus.com/bid/48157>

* SECTRACK: 1025642

<http://www.securitytracker.com/id/1025642>

CVE Reference:

CVE-2011-1272 (cve.mitre.org, nvd.nist.gov)

• 19382 Excel Improper Record Parsing Vulnerability (MS11-045/2537146) (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: MS11-045
<http://www.microsoft.com/technet/security/Bulletin/MS11-045.msp>
- * BID: 48158
<http://www.securityfocus.com/bid/48158>
- * SECTRACK: 1025642
<http://www.securitytracker.com/id/1025642>

CVE Reference:

CVE-2011-1273 (cve.mitre.org, nvd.nist.gov)

• 19383 Excel Out of Bounds Array Access Vulnerability (MS11-045/2537146) (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: MS11-045
<http://www.microsoft.com/technet/security/Bulletin/MS11-045.msp>
- * BID: 48159
<http://www.securityfocus.com/bid/48159>
- * SECTRACK: 1025642
<http://www.securitytracker.com/id/1025642>

CVE Reference:

CVE-2011-1274 (cve.mitre.org, nvd.nist.gov)

• 19384 Excel Memory Heap Overwrite Vulnerability (MS11-045/2537146) (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: MS11-045
<http://www.microsoft.com/technet/security/Bulletin/MS11-045.msp>
- * BID: 48160
<http://www.securityfocus.com/bid/48160>
- * SECTRACK: 1025642
<http://www.securitytracker.com/id/1025642>

CVE Reference:

CVE-2011-1275 (cve.mitre.org, nvd.nist.gov)

• 19385 Excel Buffer Overrun Vulnerability (MS11-045/2537146) (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: MS11-045
<http://www.microsoft.com/technet/security/Bulletin/MS11-045.msp>
* BID: 48161
<http://www.securityfocus.com/bid/48161>
* SECTRACK: 1025642
<http://www.securitytracker.com/id/1025642>

CVE Reference:

CVE-2011-1276 (cve.mitre.org, nvd.nist.gov)

• **19386 Excel Memory Corruption Vulnerability (MS11-045/2537146) (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: MS11-045
<http://www.microsoft.com/technet/security/Bulletin/MS11-045.msp>
* BID: 48162
<http://www.securityfocus.com/bid/48162>
* SECTRACK: 1025642
<http://www.securitytracker.com/id/1025642>

CVE Reference:

CVE-2011-1277 (cve.mitre.org, nvd.nist.gov)

• **19387 Excel WriteAV Vulnerability (MS11-045/2537146) (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: MS11-045
<http://www.microsoft.com/technet/security/Bulletin/MS11-045.msp>
* BID: 48163
<http://www.securityfocus.com/bid/48163>
* SECTRACK: 1025642
<http://www.securitytracker.com/id/1025642>

CVE Reference:

CVE-2011-1278 (cve.mitre.org, nvd.nist.gov)

• **19388 Excel Out of Bounds WriteAV Vulnerability (MS11-045/2537146) (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: MS11-045
<http://www.microsoft.com/technet/security/Bulletin/MS11-045.msp>
* BID: 48164
<http://www.securityfocus.com/bid/48164>
* SECTRACK: 1025642
<http://www.securitytracker.com/id/1025642>

CVE Reference:

CVE-2011-1279 (cve.mitre.org, nvd.nist.gov)

• **19389 DFS Memory Corruption Vulnerability (MS11-042/2535512) (Remote File Checking)**

An unauthenticated remote code execution vulnerability exists in the way that the Distributed File System (DFS) client parses specially crafted DFS responses. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted DFS response to a client-initiated DFS request. An attacker who successfully exploited this vulnerability could execute arbitrary code and 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: MS11-042
<http://www.microsoft.com/technet/security/Bulletin/MS11-042.msp>
- * BID: 48180
<http://www.securityfocus.com/bid/48180>
- * SECTRACK: 1025639
<http://www.securitytracker.com/id/1025639>

CVE Reference:

CVE-2011-1868 (cve.mitre.org, nvd.nist.gov)

• **19390 DFS Referral Response Vulnerability (MS11-042/2535512) (Remote File Checking)**

A denial of service vulnerability exists in the way that Microsoft Distributed File System (DFS) handles specially crafted DFS referral responses. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service.

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

References:

- * MS: MS11-042
<http://www.microsoft.com/technet/security/Bulletin/MS11-042.msp>
- * BID: 48187
<http://www.securityfocus.com/bid/48187>
- * SECTRACK: 1025639
<http://www.securitytracker.com/id/1025639>

CVE Reference:

CVE-2011-1869 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2011-2204 Apache CVSS 2.0 Score = 1.9**

Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.17, when the MemoryUserDatabase is used, creates log entries containing passwords upon encountering errors in JMX user creation, which allows local users to obtain sensitive information by reading a log file.

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

- CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=717013
- XF: <http://xforce.iss.net/xforce/xfdb/68238>
- BID: <http://www.securityfocus.com/bid/48456>
- OSVDB: <http://www.osvdb.org/73429>
- CONFIRM: <http://tomcat.apache.org/security-7.html>
- CONFIRM: <http://tomcat.apache.org/security-6.html>
- CONFIRM: <http://tomcat.apache.org/security-5.html>
- SECTRACK: <http://securitytracker.com/id?1025712>
- SECUNIA: <http://secunia.com/advisories/44981>

CVE Reference: [CVE-2011-2204](#)

• **CVE-2011-2349 Google CVSS 2.0 Score = 7.5**

Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to text selection.

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

References:

CONFIRM: http://googlechromereleases.blogspot.com/2011/06/stable-channel-update_28.html

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=85418>

CVE Reference: [CVE-2011-2349](#)

• **CVE-2011-2346 Google CVSS 2.0 Score = 7.5**

Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG fonts.

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

References:

CONFIRM: http://googlechromereleases.blogspot.com/2011/06/stable-channel-update_28.html

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=84355>

CVE Reference: [CVE-2011-2346](#)

• **CVE-2011-2351 Google CVSS 2.0 Score = 7.5**

Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG use elements.

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

References:

CONFIRM: http://googlechromereleases.blogspot.com/2011/06/stable-channel-update_28.html

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=85211>

CVE Reference: [CVE-2011-2351](#)

• **CVE-2011-2350 Google CVSS 2.0 Score = 7.5**

The HTML parser in Google Chrome before 12.0.742.112 does not properly address "lifetime and re-entrancy issues," which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

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

References:

CONFIRM: http://googlechromereleases.blogspot.com/2011/06/stable-channel-update_28.html

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=85102>

CVE Reference: [CVE-2011-2350](#)

• **CVE-2011-2347 Google CVSS 2.0 Score = 7.5**

Google Chrome before 12.0.742.112 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.

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

References:

CONFIRM: http://googlechromereleases.blogspot.com/2011/06/stable-channel-update_28.html

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=85003>

CVE Reference: [CVE-2011-2347](#)

• **CVE-2011-2348 Google CVSS 2.0 Score = 7.5**

Google V8, as used in Google Chrome before 12.0.742.112, performs an incorrect bounds check, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

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

References:

CONFIRM: http://googlechromereleases.blogspot.com/2011/06/stable-channel-update_28.html

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=85177>

CVE Reference: [CVE-2011-2348](#)

• **CVE-2011-2345 Google CVSS 2.0 Score = 5.0**

The NPAPI implementation in Google Chrome before 12.0.742.112 does not properly handle strings, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

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

References:

CONFIRM: http://googlechromereleases.blogspot.com/2011/06/stable-channel-update_28.html

CONFIRM: <http://code.google.com/p/chromium/issues/detail?id=77493>

CVE Reference: [CVE-2011-2345](#)

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