

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

Tokenization heightens security. Guide helps after attack. E-discovery in a large organization. IE zero-day patch Tuesday.

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

• Tokenization eases merchant PCI compliance

Network World - Today, it's expected that merchants accept electronic payments and that those payments are secure with no data leaks or breaches of any kind. But the reality is many merchants don't truly understand the vulnerabilities that electronic payments present. They may think they are secure when in fact they are at risk.

The Payment Card Industry Security Standards Council (PCI SSC) has been addressing security concerns by issuing the PCI Data Security Standard (PCI DSS) and ratcheting up compliance requirements. As a response, the industry has been flooded with solutions claiming to provide heightened security for a merchant's data. Merchants often invest in these offerings out of fear, uncertainty or doubt. What most don't understand is that the solutions are not bulletproof and they still may not be able to pass an audit. Computerworld

Full Story :

http://www.computerworld.com/s/article/9174440/Tokenization_eases_merchant_PCI_compliance?source=rss_security

• Guide released to mitigate damage of cyberattacks

Two industry groups on Wednesday released a free guide that the authors hope will encourage financial executives within an organization to take the lead role in mitigating cyber-risks.

The framework, developed by the Internet Security Alliance (ISA) and the American National Standards Institute (ANSI), comes in response to the White House's release last May of the 60-day Cyberspace Policy Review. That report stated that between 2008 and 2009, American business losses due to cyberattacks grew to more than \$1 trillion in intellectual property.

The new publication, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs*, helps organizations meet one of the review's recommendations that monetary value be assigned to cyber-risks and their consequences. SC Magazine

Full Story :

http://www.scmagazineus.com/guide-released-to-mitigate-damage-of-cyberattacks/article/167149/?utm_source=feed

• Making E-discovery an Internal Function

CSO - NBC Universal is one of the largest media and entertainment companies in the world. Chief Information Security Officer Jonathan Chow and his team manage information security for several business lines within NBCU, including its broadcast and cable television to film production, online ventures and its two theme parks in Hollywood, California and Orlando, Florida. Among one of the biggest challenges in the last few years has been the incredible explosion in demand for e-discovery services, according to Chow.

Since different legal teams handle the needs of each line of business, the workflows associated with managing electronic discovery vary as well, adding another layer of complexity. And because of the growing number of cases, and increases in both the amount of electronically stored information and hours spent supporting the process, demand for e-discovery services has increased 30 to 50 percent annually. The costs were spiraling out of control and this sent Chow looking for a way to manage the process internally. Computerworld

Full Story :

http://www.computerworld.com/s/article/9174334/Making_E_discovery_an_Internal_Function?source=rss_security

• Microsoft to patch IE zero-day with emergency fix Tuesday

Computerworld - Microsoft today announced it will issue an emergency security update for Internet Explorer (IE) tomorrow to patch a zero-day vulnerability that has been used to launch drive-by attacks for at least several weeks.

Tuesday's update will be the second out-of-band update -- Microsoft's term for one outside its normal once-each-month Patch Tuesday -- in the last three months. Microsoft last shipped a rush IE update to customers in late January, to fix eight flaws, including one that had been used to attack several companies' networks, including Google's and Adobe's.

"The bulletin is being released to address attacks against customers of Internet Explorer 6 and Internet Explorer 7," said Microsoft in an updated advisory. Computerworld

Full Story :

http://www.computerworld.com/s/article/9174336/Microsoft_to_patch_IE_zero_day_with_emergency_fix_Tuesday?source=rss_security

New Vulnerabilities Tested in SecureScout

• 18741 Internet Explorer Uninitialized Memory Corruption Vulnerability (MS10-018/980182) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. If a user is logged on with administrative user rights, 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: MS10-018

<http://www.microsoft.com/technet/security/bulletin/ms10-018.mspx>

* BID: 39023

<http://www.securityfocus.com/bid/39023>

* VUPEN: VUPEN/ADV-2010-0744

<http://www.vupen.com/english/advisories/2010/0744>

* SECTRACK: 1023773

<http://securitytracker.com/alerts/2010/Mar/1023773.html>

CVE Reference:

CVE-2010-0267 (cve.mitre.org, nvd.nist.gov)

• 18742 Internet Explorer Post Encoding Information Disclosure Vulnerability (MS10-018/980182) (Remote File Checking)

An information disclosure vulnerability exists in the way that Internet Explorer handles content using specific encoding strings when submitting data. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow information disclosure if a user viewed the Web page. An attacker who successfully exploited this vulnerability could view content from the local computer or another browser window in another domain or Internet Explorer zone.

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

References:

* MS: MS10-018

<http://www.microsoft.com/technet/security/bulletin/ms10-018.msp>

* BID: 39028

<http://www.securityfocus.com/bid/39028>

* VUPEN: VUPEN/ADV-2010-0744

<http://www.vupen.com/english/advisories/2010/0744>

* SECTRACK: 1023773

<http://securitytracker.com/alerts/2010/Mar/1023773.html>

CVE Reference:

CVE-2010-0488 (cve.mitre.org, nvd.nist.gov)

• 18743 Internet Explorer Race Condition Memory Corruption Vulnerability (MS10-018/980182) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that may have been corrupted due to a race condition. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. If a user is logged on with administrative user rights, 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: MS10-018

<http://www.microsoft.com/technet/security/bulletin/ms10-018.msp>

* BID: 39026

<http://www.securityfocus.com/bid/39026>

* VUPEN: VUPEN/ADV-2010-0744

<http://www.vupen.com/english/advisories/2010/0744>

* SECTRACK: 1023773

<http://securitytracker.com/alerts/2010/Mar/1023773.html>

CVE Reference:

CVE-2010-0489 (cve.mitre.org, nvd.nist.gov)

CVE-2010-0489 (cve.mitre.org, nvd.nist.gov)

• 18744 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2010-0490) (MS10-018/980182) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. If a user is logged on with administrative user rights, 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: MS10-018
<http://www.microsoft.com/technet/security/bulletin/ms10-018.msp>
- * BID: 39031
<http://www.securityfocus.com/bid/39031>
- * VUPEN: VUPEN/ADV-2010-0744
<http://www.vupen.com/english/advisories/2010/0744>
- * SECTRACK: 1023773
<http://securitytracker.com/alerts/2010/Mar/1023773.html>

CVE Reference:

CVE-2010-0490 (cve.mitre.org, nvd.nist.gov)

• 18745 Internet Explorer HTML Object Memory Corruption Vulnerability (MS10-018/980182) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. If a user is logged on with administrative user rights, 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: MS10-018
<http://www.microsoft.com/technet/security/bulletin/ms10-018.msp>
- * BID: 39027
<http://www.securityfocus.com/bid/39027>
- * VUPEN: VUPEN/ADV-2010-0744
<http://www.vupen.com/english/advisories/2010/0744>
- * SECTRACK: 1023773
<http://securitytracker.com/alerts/2010/Mar/1023773.html>

CVE Reference:

CVE-2010-0491 (cve.mitre.org, nvd.nist.gov)

• 18746 Internet Explorer HTML Object Memory Corruption Vulnerability (CVE-2010-0492) (MS10-018/980182) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. If a user is logged on with administrative user rights, 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: MS10-018
<http://www.microsoft.com/technet/security/bulletin/ms10-018.msp>
- * BID: 39030
<http://www.securityfocus.com/bid/39030>
- * VUPEN: VUPEN/ADV-2010-0744
<http://www.vupen.com/english/advisories/2010/0744>
- * SECTRACK: 1023773
<http://securitytracker.com/alerts/2010/Mar/1023773.html>

CVE Reference:

CVE-2010-0492 (cve.mitre.org, nvd.nist.gov)

• 18747 Internet Explorer HTML Element Cross-Domain Vulnerability (MS10-018/980182) (Remote File Checking)

An information disclosure vulnerability exists in Internet Explorer that could allow script to gain access to a browser window in another domain or Internet Explorer zone. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow information disclosure if a user viewed the Web page and then drags the browser window across a second browser window.

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

References:

- * MS: MS10-018
<http://www.microsoft.com/technet/security/bulletin/ms10-018.msp>
- * BID: 39047
<http://www.securityfocus.com/bid/39047>
- * VUPEN: VUPEN/ADV-2010-0744
<http://www.vupen.com/english/advisories/2010/0744>
- * SECTRACK: 1023773
<http://securitytracker.com/alerts/2010/Mar/1023773.html>

CVE Reference:

CVE-2010-0494 (cve.mitre.org, nvd.nist.gov)

• 18748 Internet Explorer Memory Corruption Vulnerability (MS10-018/980182) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer manages a long URL in certain situations. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user. If a user is logged on with administrative user rights, 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: MS10-018
<http://www.microsoft.com/technet/security/bulletin/ms10-018.msp>
- * BID: 39025
<http://www.securityfocus.com/bid/39025>
- * VUPEN: VUPEN/ADV-2010-0744
<http://www.vupen.com/english/advisories/2010/0744>
- * SECTRACK: 1023773
<http://securitytracker.com/alerts/2010/Mar/1023773.html>

CVE Reference:

CVE-2010-0805 (cve.mitre.org, nvd.nist.gov)

• 18749 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2010-0806) (MS10-018/980182) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. If a user is logged on with administrative user rights, 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: MS10-018
<http://www.microsoft.com/technet/security/bulletin/ms10-018.msp>
- * BID: 38615
<http://www.securityfocus.com/bid/38615>
- * VUPEN: VUPEN/ADV-2010-0744
<http://www.vupen.com/english/advisories/2010/0744>
- * SECTRACK: 1023773
<http://securitytracker.com/alerts/2010/Mar/1023773.html>

CVE Reference:

CVE-2010-0806 (cve.mitre.org, nvd.nist.gov)

• **18750 Internet Explorer HTML Rendering Memory Corruption Vulnerability (MS10-018/980182) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. If a user is logged on with administrative user rights, 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: MS10-018
<http://www.microsoft.com/technet/security/bulletin/ms10-018.msp>
- * BID: 39024
<http://www.securityfocus.com/bid/39024>
- * VUPEN: VUPEN/ADV-2010-0744
<http://www.vupen.com/english/advisories/2010/0744>
- * SECTRACK: 1023773
<http://securitytracker.com/alerts/2010/Mar/1023773.html>

CVE Reference:

CVE-2010-0807 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2010-1175 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 7.0 on Windows XP and Windows Server 2003 allows remote attackers to have an unspecified impact via a certain XML document that references a crafted web site in the SRC attribute of an image element, related to a "0day Vulnerability."

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

References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/510280/100/0/threaded>

CVE Reference: [CVE-2010-1175](http://cve.mitre.org/cve/2010/1175)

• **CVE-2010-0267 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6, 6 SP1, and 7 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability."

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0744>

BID: <http://www.securityfocus.com/bid/39023>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-018.msp>

SECTRACK: <http://securitytracker.com/id?1023773>

CVE Reference: [CVE-2010-0267](http://cve.mitre.org/cve/2010/0267)

• **CVE-2010-0489 Microsoft CVSS 2.0 Score = 9.3**

Race condition in Microsoft Internet Explorer 5.01 SP4, 6, 6 SP1, and 7 allows remote attackers to execute arbitrary code via a crafted HTML document that triggers memory corruption, aka "Race Condition Memory Corruption Vulnerability."

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0744>

BID: <http://www.securityfocus.com/bid/39026>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-018.msp>

SECTRACK: <http://securitytracker.com/id?1023773>

CVE Reference: [CVE-2010-0489](#)

• CVE-2010-0490 Microsoft CVSS 2.0 Score = 9.3

Microsoft Internet Explorer 6, 6 SP1, 7, and 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability."

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0744>

BID: <http://www.securityfocus.com/bid/39031>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-018.msp>

SECTRACK: <http://securitytracker.com/id?1023773>

CVE Reference: [CVE-2010-0490](#)

• CVE-2010-0491 Microsoft CVSS 2.0 Score = 9.3

Use-after-free vulnerability in Microsoft Internet Explorer 5.01 SP4, 6, and 6 SP1 allows remote attackers to execute arbitrary code by changing unspecified properties of an HTML object that has an onreadystatechange event handler, aka "HTML Object Memory Corruption Vulnerability."

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0744>

BID: <http://www.securityfocus.com/bid/39027>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-018.msp>

SECTRACK: <http://securitytracker.com/id?1023773>

IDEFENSE: <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=864>

CVE Reference: [CVE-2010-0491](#)

• CVE-2010-0492 Microsoft CVSS 2.0 Score = 9.3

mstime.dll in Microsoft Internet Explorer 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "HTML Object Memory Corruption Vulnerability."

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0744>

BID: <http://www.securityfocus.com/bid/39030>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-018.msp>

SECTRACK: <http://securitytracker.com/id?1023773>

CVE Reference: [CVE-2010-0492](#)

• CVE-2010-0805 Microsoft CVSS 2.0 Score = 9.3

The Tabular Data Control (TDC) ActiveX control in Microsoft Internet Explorer 5.01 SP4, 6 on Windows XP SP2 and SP3, and 6 SP1 allows remote attackers to execute arbitrary code via a long URL that triggers memory corruption, aka "Memory Corruption Vulnerability."

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0744>

BID: <http://www.securityfocus.com/bid/39025>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-018.msp>

SECTRAK: <http://securitytracker.com/id?1023773>

CVE Reference: [CVE-2010-0805](#)

• **CVE-2010-0807 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 7 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing a deleted object, leading to memory corruption, aka "HTML Rendering Memory Corruption Vulnerability."

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2010/0744>

BID: <http://www.securityfocus.com/bid/39024>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-018.msp>

SECTRAK: <http://securitytracker.com/id?1023773>

CVE Reference: [CVE-2010-0807](#)

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