Check Point
SOFTWARE TECHNOLOGIES LTD.

Threat Intelligence & Research

THREAT PREVENTION COVERAGE TOP 30 HIGH RISK VULNERABILITIES

OVERVIEW

- Cyber threat actors continue to exploit unpatched software to conduct attacks against critical infrastructure organizations.
- The US-CERT has issued an alert which provides information on the 30 most commonly exploited vulnerabilities used in these attacks.
- The alert is based on analysis completed by the Canadian Cyber Incident Response Centre (CCIRC) and was developed in collaboration with partners from Canada, New Zealand, the United Kingdom, and the Australian Cyber Security Centre.

- **THIS DOCUMENT WILL LIST CHECK POINT'S PROTECTIONS ADDRESSING THESE TOP 30 VULNERABILITIES**

ATTACKS & VULNERABILITIES IMPACT

Unpatched vulnerabilities allow malicious actors entry points into a network. A set of vulnerabilities are consistently targeted in observed attacks

A successful network intrusion can have severe impacts, particularly if the compromise becomes public and sensitive information is exposed. Possible impacts include:

- Temporary or permanent loss of sensitive or proprietary information.
- Disruption to regular operations.
- Financial losses relating to restoring systems and files.
- Potential harm to an organization's reputation.

LIST OF RELEVANT IPS PROTECTIONS

Vendor	Vulnerability	IPS Protection
Microsoft	CVE-2006-3227	Internet Explorer US-ASCII Charset Obfuscation
Microsoft	CVE-2008-2244	Microsoft Word Crafted SmartTag Record Code Execution (MS08-042)
Microsoft	CVE-2009-3129	Microsoft Office Excel Featheader Record Memory Corruption (MS09-067)
Microsoft	CVE-2009-3674	Internet Explorer 8 Circular References Memory Corruption (MS09-072)

©2015 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

Microsoft	CVE-2010-0806	Internet Explorer iepeers.dll Remote Code Execution
Microsoft	CVE-2010-3333	Microsoft Office RTF Stack Buffer Overflow (MS10-087)
Microsoft	CVE-2011-0101	Microsoft Office Excel RealTimeData Record Memory Corruption (MS11-021)
Microsoft	CVE-2012-0158	Microsoft MSCOMCTL.OCX ActiveX Control Remote Code Execution (MS12-027)
Microsoft	CVE-2012-1856	Microsoft Windows Common Controls Remote Code
Microsoft	CVE-2012-4792	Internet Explorer Heap Spray Memory Corruption
Microsoft	CVE-2013-0074	Microsoft Silverlight Pointer Dereference Memory
Microsoft	CVE-2013-1347	Microsoft Internet Explorer 8 Use After Free Code Execution - Zero Day
Microsoft	CVE-2014-0322	Microsoft Internet Explorer Use-After-Free Code Execution
Microsoft	CVE-2014-1761	Microsoft Word RTF listoverridecount Memory Corruption
Microsoft	CVE-2014-1776	Microsoft Internet Explorer Remote Code Execution (CVE-2014-1776)
Microsoft	CVE-2014-4114	Microsoft Windows OLE Remote Code Execution (MS14-060)
Adobe	CVE-2009-3953	A protection for this vulnerability is currently under development
Adobe	CVE-2010-0188	Adobe Reader Libtiff TIFFFetchShortPair Stack Buffer
Adobe	CVE-2010-2883	Adobe Reader and Acrobat TTF SING Table Buffer Overflow (APSA10-02)
Adobe	CVE-2011-0611	Adobe Flash Player ActionScript callMethod Code Execution (APSA11-02)
Adobe	CVE-2011-2462	Adobe Reader and Acrobat U3D Shading Modifier Memory Corruption (APSA11-04)
Adobe	CVE-2013-0625	Adobe ColdFusion scheduleedit.cfm Authentication Bypass
Adobe	CVE-2013-0632	Adobe ColdFusion Authentication Bypass
Adobe	CVE-2013-2729	Adobe Acrobat Reader Crafted RLE8 format BMP File Buffer Overflow (APSB13-15)
Adobe	CVE-2013-3336	Adobe ColdFusion Directory Traversal Information Disclosure (APSA13-03)
Adobe	CVE-2013-5326	There is currently no protection for this vulnerability
Adobe	CVE-2014-0564	Adobe Flash Player Memory Corruption (APSB14-22: CVE-2014-0564)
Oracle	CVE-2012-1723	Oracle Java Runtime Bytecode Verifier Cache Code Execution
Oracle	CVE-2013-2465	Oracle Java Runtime Environment storeImageArray Buffer Overflow
OpenSSL	CVE-2014-0160	OpenSSL TLS Heartbeat information disclosure

©2015 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

REFERENCES

US-CERT Alert (TA-15-119A): https://www.us-cert.gov/ncas/alerts/TA15-119A
Vulnerability Details: https://web.nvd.nist.gov

©2015 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content