Systems Affected

Systems running unpatched software from Adobe, Microsoft, Oracle, or OpenSSL.

Overview

Cyber threat actors continue to exploit unpatched software to conduct attacks against critical infrastructure organizations. As many as 85 percent of targeted attacks are preventable [1](link is external).

This Alert provides information on the 30 most commonly exploited vulnerabilities used in these attacks, along with prevention and mitigation recommendations.

It is based on analysis completed by the Canadian Cyber Incident Response Centre (CCIRC) and was developed in collaboration with our partners from Canada, New Zealand, the United Kingdom, and the Australian Cyber Security Centre.

Description

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

Impact

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, and
- Potential harm to an organization's reputation.

Solution

Maintain up-to-date software

The attack vectors frequently used by malicious actors such as email attachments, compromised "watering hole" websites, and other tools often rely on taking advantage of unpatched vulnerabilities found in widely used software applications. Patching is the process of repairing vulnerabilities found in these software components.

It is necessary for all organizations to establish a strong ongoing patch management process to ensure the proper preventive measures are taken against potential threats. The longer a system remains unpatched, the longer it is vulnerable to being compromised. Once a patch has been publicly released, the underlying vulnerability can be reverse engineered by malicious actors in order to create an exploit. This process has been documented to take anywhere from 24-hours to four days. Timely patching is one of the lowest cost yet most effective steps an organization can take to minimize its exposure to the threats facing its network.

Patch commonly exploited vulnerabilities

Executives should ensure their organization's information security professionals have patched the following software vulnerabilities. Please see patching information for version specifics.

CVE	Affected Products	Patching Information
06-3227	Internet Explorer	Microsoft Malware Protection Encyclopedia Entry(link is external)
08-2244	Office Word	Microsoft Security Bulletin MS08-042(link is external)

CVE	Affected Products	Patching Information
09-3129	Office Office for Mac Open XML File Format Converter for Mac Office Excel Viewer Excel Office Compatibility Pack for Word, Excel, and PowerPoint	Microsoft Security Bulletin MS09-067(link is external)
09-3674	Internet Explorer	Microsoft Security Bulletin MS09-072(link is external)
10-0806	Internet Explorer	Microsoft Security Bulletin MS10-018(link is external)
10-3333	Office Office for Mac Open XML File Format Converter for Mac	Microsoft Security Bulletin MS10-087(link is external)
11-0101	Excel	Microsoft Security Bulletin MS11-021(link is external)
12-0158	Office SQL Server BizTalk Server Commerce Server Visual FoxPro Visual Basic	Microsoft Security Bulletin MS12-027(link is external)
12-1856	Office SQL Server Commerce Server Host Integration Server Visual FoxPro Visual Basic	Microsoft Security Bulletin MS12-060(link is external)
12-4792	Internet Explorer	Microsoft Security Bulletin MS13-008(link is external)
13-0074	Silverlight and Developer Runtime	Microsoft Security Bulletin MS13-022(link is external)

CVE	Affected Products	Patching Information
13-1347	Internet Explorer	Microsoft Security Bulletin MS13-038(link is external)
14-0322	Internet Explorer	Microsoft Security Bulletin MS14-012(link is external)
14-1761	Microsoft Word Office Word Viewer Office Compatibility Pack Office for Mac Word Automation Services on SharePoint Server Office Web Apps Office Web Apps Server	Microsoft Security Bulletin MS14-017(link is external)
14-1776	Internet Explorer	Microsoft Security Bulletin MS14-021(link is external)
14-4114	Windows	Microsoft Security Bulletin MS14-060(link is external)

Microsoft

CVE	Affected Products	Patching Information
12-1723	Java Development Kit, SDK, and JRE	Oracle Java SE Critical Patch Update Advisory - June 2012(lin external)
13-2465	Java Development Kit and JRE	Oracle Java SE Critical Patch Update Advisory - June 2013(lin external)

Oracle

CVE	Affected Products	Patching Information
09-3953	Reader Acrobat	Adobe Security Bulletin APSB10-02(link is external
10-0188	Reader Acrobat	Adobe Security Bulletin APSB10-07(link is external
10-2883	Reader Acrobat	Adobe Security Bulletin APSB10-21(link is external
11-0611	Flash Player AIR Reader Acrobat	Adobe Security Bulletin APSB11-07(link is external Adobe Security Bulletin APSB11-08(link is external
11-2462	Reader Acrobat	Adobe Security Bulletin APSB11-30(link is external
13-0625	ColdFusion	Adobe Security Bulletin APSB13-03(link is external
13-0632	ColdFusion	Adobe Security Bulletin APSB13-03(link is external
13-2729	Reader Acrobat	Adobe Security Bulletin APSB13-15(link is external
13-3336	ColdFusion	Adobe Security Bulletin APSB13-13(link is external
13-5326	ColdFusion	Adobe Security Bulletin APSB13-27(link is external
14-0564	Flash Player AIR AIR SDK & Compiler	Adobe Security Bulletin APSB14-22(link is external

Adobe

CVE	Affected Products	Patching Information
14-0160	OpenSSL	CERT Vulnerability Note VU#720951

CVE	Affected Products	Patching Information
	OpenSSL	

Implement the following four mitigation strategies.

As part of a comprehensive security strategy, network administrators should implement the following four mitigation strategies, which can help prevent targeted cyber attacks.

g	Mitigation Strategy	Rationale
	Use **application whitelisting** to help prevent malicious software and unapproved programs from running.	Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious sof
	Patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office.	Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the numbe exploitable entry points available to an attacker.
	Patch operating system vulnerabilities.	
	Restrict administrative privileges to operating systems and applications based on user duties.	Restricting these privileges may prevent malware from running or limit its c to spread through the network.

It is recommended that users review US-CERT Security Tip (ST13-003) and CCIRC's Mitigation Guidelines for Advanced Persistent Threats(link is external) for additional background information and to assist in the detection of, response to, and recovery from malicious activity linked to advance persistent threats [2(link is external), 3].

References

- [1] Canadian Cyber Incident Response Centre, Top 4 Strategies to Mitigate Targeted Cyber Intrusions(link is external)
- [2] Canadian Cyber Incident Response Centre, TR11-002, Mitigation Guidelines for Advanced Persistent Threats(link is external)
- [3] US-CERT Security Tip (ST13-003): Handling Destructive Malware

Revisions

- April 29, 2015: Initial release