**Skills Assessment**

Gihan Shamike Liyanage

Information Security Management

1142109

1. A vulnerability is a weakness in a system or network that can be exploited by an attacker to gain unauthorized access or perform malicious actions. An exposure is the state of being exposed or at risk to a particular threat. An exposure can be a potential vulnerability that has not been exploited yet.
2. Top Vulnerabilities

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Vendor Name** | **#Vulnerabilities** | **#Products** |
| 1 | Microsoft | 13 | 365 apps  Access  Azure  Asp.net Core  Asp.net Model View Controller  Asp.net Mvc  Asp.net Signalr |
| 2 | Oracle | 9 | 10g Enterprise Manager Database Control  10g Enterprise Manager Grid Control  10g Reports Server  Access Manager  Adaptive Access Manager  Advanced Collections |
| 3 | Google | 56 | Android Api  Android Sdk Platform Tools  Gmail  Earth  Firebase Php-jwt  Chrome |
| 4 | Debian | 70 | Apache  Advanced Package Too  Debian Linux  Dpkg |
| 5 | Apple | 42 | Apple TV  Darwin Streaming Server  Icloud |
| 6 | IBM | 4 | AIX  Algo one  Filenet  Filenet Content Manager  Filenet P8 Application Engine  Financial Transaction Manager For Multiplatform |

(cvedetails, n.d.)

1. Security Update for Adobe Flash Player (4014329)

This security update resolves vulnerabilities in Adobe Flash Player when installed on all supported editions of Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, Windows 10, and Windows Server 2016.

This security update is rated Critical. The update addresses the vulnerabilities in Adobe Flash Player by updating the affected Adobe Flash libraries contained within Internet Explorer 10, Internet Explorer 11, and Microsoft Edge. For more information, see the Affected Software section.

**Recommended Actions**

You can disable attempts to instantiate Adobe Flash Player in Internet Explorer and other applications that honor the kill bit feature, such as Office 2007 and Office 2010, by setting the kill bit for the control in the registry.

**Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

To set the kill bit for the control in the registry, perform the following steps:

* 1. Paste the following into a text file and save it with the .reg file extension.

Windows Registry Editor Version 5.00

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}]

"Compatibility Flags"=dword:00000400

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}]

"Compatibility Flags"=dword:00000400

* 1. Double-click the .reg file to apply it to an individual system. You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection.

**Note** You must restart Internet Explorer for your changes to take effect.

**Impact of workaround**. There is no impact as long as the object is not intended to be used in Internet Explorer.

**How to undo the workaround.** Delete the registry keys that were added in implementing this workaround.

(Microsoft Security Bulletin MS17-023 - Critical, n.d.)

1. **Common Name** - Directory Traversal Elevation of Privilege Vulnerability

**CVE Identifier** - CVE-2015-0016

This security update resolves a privately reported vulnerability in Windows Error Reporting (WER). The vulnerability could allow security feature bypass if successfully exploited by an attacker. An attacker who successfully exploited this vulnerability could gain access to the memory of a running process. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Basically, it is a Security Feature Bypass (Microsoft Security Bulletin, n.d.).

1. **Precautions**

They recommend installing update 2919355 on your Windows RT 8.1-based, Windows 8.1-based, or Windows Server 2012 R2-based computer so that you receive updates in the future. But if you install a language pack after you install this update, you must reinstall this update.

**If Already Vulnerable**

Remove TSWbPrxy from the IE Elevation Policy

Note Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. For information about how to edit the registry, view the "Changing Keys And Values" Help topic in Registry Editor (Regedit.exe) or view the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe.

Using Registry Editor:

1. Click Start, click Run, type Regedit in the Open box, and then click OK.
2. In the Registry Editor locate and then select the following registry key:
3. HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Low Rights\ElevationPolicy
4. Select {B43A0C1E-B63F-4691-B68F-CD807A45DA01}
5. Click the File menu and select Export.
6. In the ExportRegistryFile dialog box type “tswebproxy\_configuration\_backup.reg” and click Save.
7. Right-click {B43A0C1E-B63F-4691-B68F-CD807A45DA01} and click Delete.
8. Click OK.

Impact of workaround. TSWbPrxy.exe will not run from within the Internet Explorer Sandbox.

(Microsoft Security Bulletin, n.d.)

1. **Common Name** - Windows Telnet Service Buffer Overflow Vulnerability.

**CVE Identifier** - CVE-2015-0014.

The vulnerability could allow remote code execution if an attacker sends specially crafted packets to an affected Windows server. Only customers who enable this service are vulnerable. By default, Telnet is installed but not enabled on Windows Server 2003. Telnet is not installed by default on Windows Vista and later operating systems (Microsoft Security Bulletin, n.d.).

1. **Precautions**

Download the updates for your home computer or laptop from the Microsoft Update website.

Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.

**If already vulnerable**

Microsoft has not identified any workarounds for this vulnerability (Vulnerability in Windows Telnet Service Could Allow Remote Code Execution (3020393), n.d.).

1. Current Threat Level: **Green**
2. WannaCry Ransomware Worm.

The ransomware was first noticed on Friday and spread very quickly through many large organizations worldwide [verge]. Unlike prior ransomware, this sample used the SMBv1 “ETERNALBLUE” exploit to spread. “ETERNALBLUE” became public about a month ago when it was published as part of the Shadowbroker archive of NSA hacking tools [shadow].

A month prior to the release of the hacking tool, Microsoft had patched the vulnerability as part of the March Patch Tuesday release. The patch was released for Windows Vista, Windows Server 2008 and later versions of Windows as part of MS17-010 in March [MS17-010]. In response to the rapid spread of WannaCry, on Friday Microsoft released a patch for older versions of Windows, going back to Windows XP and Windows Server 2003 [msft].

At the time of the initial WannaCry outbreak, we also noticed a significant increase in scanning for port 445 [port445]. The increase was likely caused by infected systems scanning for more victims. It is not clear how the infection started. There are some reports of e-mails that include the malware as attachment seeding infected networks. But at this point, no actual samples have been made public. It is possible that the worm entered a corporate network via vulnerable hosts that had port 445 exposed to the internet. The WannaCry malware itself does have no e-mail component.

1. (a) OpenSSL Heartbleed.

For those of you using OpenSSL 1.0.1 (most recent Unix systems), it is critical that you patch the openssl library, as well as binaries compiled statically with openssl, as soon as possible. [1]

The attack will allow a remote attacker to read up to 64kBytes of system memory from your system per attack attempt. The attack works against servers as well as against clients. While not all software using SSL necessarily uses the OpenSSL library, many do. (see our prior diary)

A proof of concept exploit has been made available and I have tested it. It can be used to remotely scan for vulnerable systems. [1] We have not yet detected wide spread use of the exploit, but it is literally hours old. At this point, we don't think the vulnerability was known in the underground before the official release, but it is possible.

**Prevention if You are Vulnerable**

Patch! Ubuntu, CentOS and others have patches available. OS X Mavericks has NO PATCH available. Windows is likely not vulnerable, but if you are running open source software like Apache that uses OpenSSL, then you may be vulnerable.

You may want to consider replacing SSL certificates if you are afraid that the exploit was already used against your site. But the exploit is not limited to secret SSL key. All data in memory is potentially at risk.

(b) Account has been created

A screenshot of a computer

Description automatically generated with medium confidence

**Reference**

*cvedetails*. (n.d.). Retrieved from cvedetails: https://www.cvedetails.com/

*Internet Storm Center*. (n.d.). Retrieved from Internet Storm Center: https://isc.sans.edu/

*Microsoft Security Bulletin*. (n.d.). Retrieved from Microsoft Security Bulletin: http://technet.microsoft.com/en-us/security/bulletin

*Microsoft Security Bulletin MS17-023 - Critical*. (n.d.). Retrieved from Microsoft Security Bulletin MS17-023 - Critical: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-023

*Vulnerability in Windows Telnet Service Could Allow Remote Code Execution (3020393)*. (n.d.). Retrieved from Tenable: https://www.tenable.com/plugins/nessus/80491