**1.1. Microsoft Office 365 Unsupported Channel Version Detection**

|  |  |
| --- | --- |
| **Rick Score:** | Critical |
| **Affected Systems:** | https://192.168.100.150 |

**1.1.1. Vulnerability Description**

According to its Channel version, the installation of Microsoft Office 365 on the remote Windows host is no longer supported.  
  
Once a new version of the Monthly Channel or the Semi-annual Channel (Targeted) is released, the previous version is no longer supported.  
Only the two latest versions of the Semi-annual Channel are supported.  
The semi-annual feature update releases of Office 365 ProPlus are supported for 18 months, starting from the initial release.  
A new version, with feature updates, will be released to Semi-Annual Channel (Targeted) in March and September. Four months later, in July and January, that version, with those feature updates, will be released to Semi-Annual Channel and will be supported for the next 14 months.  
  
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

**1.1.3. Evidence**

**1.1.3. Recommendation**

Upgrade to a Channel version of Microsoft Office 365 that is currently supported.

**1.1.4. References**

https://docs.microsoft.com/en-us/officeupdates/update-history-office365-proplus-by-date?redirectSourcePath=%252fen-us%252farticle%252fae942449-1fca-4484-898b-a933ea23def7  
http://www.nessus.org/u?cebfe0cb

**1.2. Internet Explorer Scripting Engine Memory Corruption Vulnerability (CVE-2020-0674)**

|  |  |
| --- | --- |
| **Rick Score:** | High |
| **Affected Systems:** | https://192.168.100.150 |
| **CVSS Risk Score:** | CVE-2020-0674 |

**1.2.1. Vulnerability Description**

The Internet Explorer installation on the remote host is missing a security update. It is, therefore, affected by the following vulnerability :  
  
 - A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2020-0674)

**1.2.3. Evidence**

**1.2.3. Recommendation**

Refer to mitigation steps in Microsoft advisory ADV200001.

**1.2.4. References**

http://www.nessus.org/u?0ef3f446

**1.3. MS09-035: Vulnerabilities in Visual Studio Active Template Library Could Allow Remote Code Execution (969706)**

|  |  |
| --- | --- |
| **Rick Score:** | High |
| **Affected Systems:** | https://192.168.100.150 |
| **CVSS Risk Score:** | CVE-2009-0901 |

**1.3.1. Vulnerability Description**

The remote Windows host contains a version of the Microsoft Active Template Library (ATL), included as part of Visual Studio or Visual C++, that is affected by multiple vulnerabilities :  
  
 - On systems with components and controls installed that were built using Visual Studio ATL, an issue in the ATL headers could allow an attacker to force VariantClear to be called on a VARIANT that has not been correctly initialized and, by supplying a corrupt stream, to execute arbitrary code. (CVE-2009-0901)  
  
 - On systems with components and controls installed that were built using Visual Studio ATL, unsafe usage of OleLoadFromStream could allow instantiation of arbitrary objects that can bypass related security policy, such as kill bits within Internet Explorer.  
 (CVE-2009-2493)  
  
 - On systems with components and controls installed that were built using Visual Studio ATL, an issue in the ATL headers could allow a string to be read without a terminating NULL character, which could lead to disclosure of information in memory. (CVE-2009-2495)

**1.3.3. Evidence**

**1.3.3. Recommendation**

Microsoft has released a set of patches for Visual Studio .NET 2003, Visual Studio 2005 and 2008, as well as Visual C++ 2005 and 2008.

**1.3.4. References**

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2009/ms09-035

**1.4. MS11-025: Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution (2500212)**

|  |  |
| --- | --- |
| **Rick Score:** | High |
| **Affected Systems:** | https://192.168.100.150 |
| **CVSS Risk Score:** | CVE-2010-3190 |

**1.4.1. Vulnerability Description**

The remote Windows host contains a version of the Microsoft Foundation Class (MFC) library affected by an insecure library loading vulnerability. The path used for loading external libraries is not securely restricted.  
  
An attacker can exploit this by tricking a user into opening an MFC application in a directory that contains a malicious DLL, resulting in arbitrary code execution.

**1.4.3. Evidence**

**1.4.3. Recommendation**

Microsoft has released a set of patches for Visual Studio .NET 2003, 2005, and 2008, as well as Visual C++ 2005, 2008, and 2010.

**1.4.4. References**

http://www.nessus.org/u?e2e88505

**1.5. Microsoft Windows Unquoted Service Path Enumeration**

|  |  |
| --- | --- |
| **Rick Score:** | Medium |
| **Affected Systems:** | https://192.168.100.150 |
| **CVSS Risk Score:** | CVE-2013-1609 |

**1.5.1. Vulnerability Description**

The remote Windows host has at least one service installed that uses an unquoted service path, which contains at least one whitespace. A local attacker can gain elevated privileges by inserting an executable file in the path of the affected service.  
  
Note that this is a generic test that will flag any application affected by the described vulnerability.

**1.5.3. Evidence**

**1.5.3. Recommendation**

Ensure that any services that contain a space in the path enclose the path in quotes.

**1.5.4. References**

http://www.nessus.org/u?84a4cc1c  
http://cwe.mitre.org/data/definitions/428.html  
https://www.commonexploits.com/unquoted-service-paths/  
http://www.nessus.org/u?4aa6acbc

**1.6. SMB Signing not required**

|  |  |
| --- | --- |
| **Rick Score:** | Medium |
| **Affected Systems:** | https://192.168.100.150 |

**1.6.1. Vulnerability Description**

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**1.6.3. Evidence**

**1.6.3. Recommendation**

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

**1.6.4. References**

https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing  
http://technet.microsoft.com/en-us/library/cc731957.aspx  
http://www.nessus.org/u?74b80723  
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html  
http://www.nessus.org/u?a3cac4ea

**1.7. Windows Speculative Execution Configuration Check**

|  |  |
| --- | --- |
| **Rick Score:** | Medium |
| **Affected Systems:** | https://192.168.100.150 |
| **CVSS Risk Score:** | CVE-2017-5715 |

**1.7.1. Vulnerability Description**

The remote host has not properly mitigated a series of known speculative execution vulnerabilities. It, therefore, may be affected by :  
 - Branch Target Injection (BTI) (CVE-2017-5715)  
 - Bounds Check Bypass (BCB) (CVE-2017-5753)  
 - Rogue Data Cache Load (RDCL) (CVE-2017-5754)  
 - Rogue System Register Read (RSRE) (CVE-2018-3640)  
 - Speculative Store Bypass (SSB) (CVE-2018-3639)  
 - L1 Terminal Fault (L1TF) (CVE-2018-3615, CVE-2018-3620, CVE-2018-3646)  
 - Microarchitectural Data Sampling Uncacheable Memory (MDSUM) (CVE-2019-11091)  
 - Microarchitectural Store Buffer Data Sampling (MSBDS) (CVE-2018-12126)  
 - Microarchitectural Load Port Data Sampling (MLPDS) (CVE-2018-12127)  
 - Microarchitectural Fill Buffer Data Sampling (MFBDS) (CVE-2018-12130)  
 - TSX Asynchronous Abort (TAA) (CVE-2019-11135)

**1.7.3. Evidence**

**1.7.3. Recommendation**

Apply vendor recommended settings.

**1.7.4. References**

http://www.nessus.org/u?8902cebb  
http://www.nessus.org/u?6a005ed4