VULNERABILITY ANALYSIS

ISEC2076

Assignment #2

Steylen, Lucas
W0459874

Uncredentialed Scan

With an Uncredentialed Nessus Scan I was able to detect 1 high vulnerability and 6 different Medium Vulnerabilities between the two machines. Below is a list and description of each vulnerability found with the Uncredentialed Scan.

High Vulnerabilities

SSL Medium Strength Cipher Suites Supported (SWEET32)

The remote host is compatible with SSL ciphers providing encryption of moderate strength. Nessus defines medium strength encryption as encryption employing key lengths between 64 bits and 112 bits or using the 3DES encryption suite. It is much easier to defeat medium strength encryption.

CVSS v3.0 Base Score: 7.5

Referenced CVEs: CVE-2016-2183

Medium Vulnerabilities

SSL Certificate Cannot Be Trusted

The server's X.509 certificate may be untrustworthy in three ways:

1. The certificate chain isn't linked to a recognized authority, possibly due to a self-signed top certificate or missing intermediates.
2. It may contain an expired certificate, either pre- or post-validity dates.

3. The certificate chain could feature an invalid signature, not matching the certificate's details or using unrecognizable signing algorithms. This disrupts user verification, potentially enabling man-in-the-middle attacks on a public, production host.

CVSS v3.0 Base Score: 6.5

SSL Self-Signed Certificate

The X.509 certificate chain for this service lacks a signature from a reputable certificate authority. If the remote host is a publicly used production server, this renders SSL ineffective, making it potentially vulnerable to man-in-the-middle attacks.

CVSS v3.0 Base Score: 6.5

TLS Version 1.0 Protocol Detection

The remote service supports TLS 1.0 encryption, which is known to have cryptographic design flaws. While modern TLS 1.0 implementations address some of these issues, it's recommended to use newer TLS versions such as 1.2 and 1.3 whenever possible, as they are designed to be more resilient against these vulnerabilities.

CVSS v3.0 Base Score: 6.5

TLS Version 1.1 Protocol Deprecated

The remote service allows connections encrypted with TLS 1.1, which does not support current or recommended cipher suites. It's unable to use ciphers that support encryption before MAC computation and authenticated encryption modes like GCM.
CVSS v3.0 Base Score: 6.5

SMB Signing not required

SMB does not require Signing on the remote server. An attacker that is unauthenticated can exploit this to remotely perform a man-in-the-middle attack against the server.

CVSS v3.0 Base Score: 5.3

SSL Certificate with Wrong Hostname

The CN attribute of the presented SSL certificate is for a different machine.

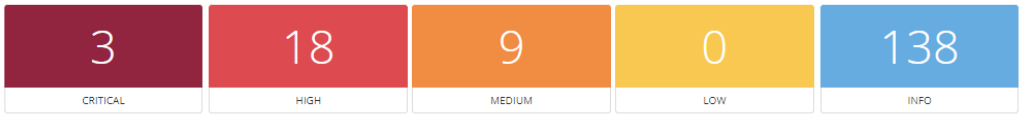
CVSS v3.0 Base Score: 5.3

Credentialed Scan

172.16.136.104

Show

172.16.137.8



Show

With a Credentialed Nessus Scan quite a few more vulnerabilities were detected. With 5 different critical vulnerabilities 22 different High and 13 different Medium. Below is a list of the most Interesting or important vulnerabilities found in each severity level.

Critical Vulnerabilities

KB5031356: Windows 10 Version 21H2 / Windows 10 Version 22H2 Security Update

The windows host is lacking essential security update 5031356 and is consequently exposed to various vulnerabilities.

1. A vulnerability related to the HTTP/2 protocol that allows for a denial of service by rapidly resetting multiple streams, as observed being exploited from August through October 2023 (CVE-2023-44487).
2. A Microsoft WDAC OLE DB provider for SQL Server vulnerability that can potentially lead to remote code execution (CVE-2023-36577).
3. An elevation of privilege vulnerability affecting Windows IIS Server (CVE-2023-36434).

CVSS v3.0 Base Score: 9.8

CVSS v3.0 Temporal Score: 9.1

Referenced CVEs: CVE-2023-44487, CVE-2023-36577, CVE-2023-36434

Mozilla Firefox < 118.0

earlier version of Firefox, predating 118.0. This means it's susceptible to multiple vulnerabilities outlined in the mfsa2023-41 advisory: A compromised content process might have supplied malicious data. leading to a potential crash in a privileged process (CVE-2023-5168).

Another vulnerability involves a compromised content process providing malicious data in a <code>PathRecording</code>, potentially leading to a crash in a privileged process (CVE-2023-5169).

In the context of canvas rendering, a compromised content process could unexpectedly alter a surface, causing a memory leak in a privileged process. In specific cases, this memory leak could be exploited for a sandbox escape (CVE-2023-5170).

During Ion compilation, a Garbage Collection event could result in a use-after-free situation, enabling an attacker to trigger a potentially exploitable crash (CVE-2023-5171).

A vulnerability in the Ion Engine's hashtable could result in mutation while having a live interior reference, leading to a potential exploitable crash (CVE-2023-5172).

In a unique Firefox configuration, an integer overflow may occur based on network traffic, potentially leading to an out-of-bounds write in privileged process memory. This configuration issue affects Firefox when a non-standard preference allows non-HTTPS Alternate Services (CVE-2023-5173).

If Windows fails to duplicate a handle during process creation, the sandbox code may unintentionally free a pointer twice, potentially leading to a use-after-free scenario and an exploitable crash. This bug only affects non-standard Firefox configurations on Windows. Other operating systems are not affected (CVE-2023-5174).

During process shutdown, it was possible that an exploit could be created and later used after being freed from a different codepath, potentially leading to a crash (CVE-2023-5175).

Memory safety issues were identified in Firefox 117, Firefox ESR 115.2, and Thunderbird 115.2. Some of these issues showed signs of memory corruption and, with sufficient effort, could potentially be exploited to execute arbitrary code (CVE-2023-5176).

CVSS v3.0 Base Score: 9.8

Referenced CVEs: CVE-2023-5168, CVE-2023-5169, CVE-2023-5170, CVE-2023-5171, CVE-2023-5172, CVE-2023-5173, CVE-2023-5174, CVE-2023-5175, CVE-2023-5176

High Vulnerabilities

Microsoft Teams < 1.6.0.18681 RCE

The Microsoft Teams version on the Windows host is older than 1.6.0.18681, making it vulnerable to a remote code execution threat. An unauthorized attacker can potentially exploit this vulnerability to bypass authentication and run arbitrary commands.

CVSS v3.0 Base Score 8.8

Referenced CVEs: CVE-2023-29328, CVE-2023-29330

Adobe Creative Cloud < 5.10.0 Arbitrary code execution (APSB23-21)

The Adobe Creative Cloud version installed on the remote Windows host is older than 5.10.0. Consequently, it is susceptible to a vulnerability mentioned in the APSB23-21 advisory. This vulnerability is related to an untrusted search path (CWE-426) that could potentially result in arbitrary code execution (CVE-2023-26358). If the application relies on a search path for locating vital resources, like software programs, there exists a potential risk where an attacker might alter this search path to direct it to a malicious program. Subsequently, the compromised application would execute this malicious program. This vulnerability is not limited to just programs; it can also impact any essential resource that the application places trust in. To fix this vulnerability Adobe Creative Cloud should be updated to version 5.10.0 or later.

CVSS v3.0 Base Score: 7.8

Referenced CVEs: CVE-2023-26358

Adobe Acrobat < 17.012.30249 / 20.005.30362 / 22.001.20169 Multiple Vulnerabilities (APSB22-32)

The Adobe Acrobat version on the remote Windows host is outdated, specifically older than versions 17.012.30249, 20.005.30362, or 22.001.20169. As a result, it is vulnerable to several security issues, including:

A 'Use After Free' vulnerability affecting Adobe Acrobat Reader versions 22.001.20142 and earlier, 20.005.30334 and earlier, and 17.012.30229 and earlier. This vulnerability could allow arbitrary code execution when a user opens a malicious file. (CVE-2022-34216, CVE-2022-34219, CVE-2022-34220, CVE-2022-34223, CVE-2022-34225, CVE-2022-34229, CVE-2022-34230)

An 'Out-of-Bounds Read' vulnerability in Adobe Acrobat Reader versions 22.001.20142 and earlier, 20.005.30334 and earlier, and 17.012.30229 and earlier. This vulnerability can lead to code execution by an attacker in the context of the current user after opening a crafted file. (CVE-2022-34215, CVE-2022-34222, CVE-2022-34226)

An 'Out-Of-Bounds Write' vulnerability affecting Adobe Acrobat Reader versions 22.001.20142 and earlier, 20.005.30334 and earlier, and 17.012.30229 and earlier. This vulnerability could result in arbitrary code execution when a user opens a malicious file. (CVE-2022-34217)

An 'Access of Resource Using Incompatible Type' ('Type Confusion') vulnerability in Adobe Acrobat Reader versions 22.001.20142 and earlier, 20.005.30334 and earlier, and 17.012.30229 and earlier. It may lead to arbitrary code execution when a victim opens a malicious file. (CVE-2022-34221)

An 'Access of Uninitialized Pointer' vulnerability affecting Adobe Acrobat Reader versions 22.001.20142 and earlier, 20.005.30334 and earlier, and 17.012.30229 and earlier. This vulnerability can result in arbitrary code execution after a user opens a malicious file. (CVE-2022-34228)

CVSS V3.0 Base Score: 7.8

Referenced CVEs: CVE-2022-34216, CVE-2022-34219, CVE-2022-34220, CVE-2022-34223, CVE-2022-34225, CVE-2022-34229, CVE-2022-34230, CVE-2022-34215, CVE-2022-34222, CVE-2022-34226, CVE-2022-34217

Medium Vulnerabilities

Apache Log4j 2.0 < 2.3.2 / 2.4 < 2.12.4 / 2.13 < 2.17.1 RCE

The version number reported for Apache Log4j on the remote host is 1.x, and this version is no longer receiving support. Log4j reached its end of life before 2016. Moreover, Log4j 1.x is afflicted by several vulnerabilities, including:

1. Log4j contains a SocketServer that accepts log events without proper verification of whether the objects are authorized, creating a potential attack vector that could be exploited (CVE-2019-17571).
2. The Apache Log4j SMTP appender inappropriately validates certificates with host mismatches, making it susceptible to interception through a man-in-the-middle attack, potentially leaking log messages (CVE-2020-9488).
3. The JMSSink utilizes JNDI in an unprotected manner, rendering any application using the JMSSink vulnerable if configured to reference an untrusted site or accessible to attackers (CVE-2022-23302).

The absence of support signifies that the vendor will not release new security patches for this product. Consequently, it is highly likely to contain security vulnerabilities.

CVSS v3.0 Base Score 6.6

Referenced CVEs: CVE-2021-44832

Security Update for Microsoft Visual Studio Code (June 2023)

The version of Microsoft Visual Studio Code installed on the remote Windows host is prior to 1.79.1. It is, therefore, affected by a session spoofing vulnerability. An attacker can exploit this to perform actions with the privileges of another user. Upgrading to Microsoft Visual Studio Code 1.79.1 or later will solve this vulnerability.

CVSS v3.0 Base Score 7.2

Referenced CVEs: CVE-2023-36742, CVE-2023-39956

Website Used

Plugins | Tenable®