Advanced Infrastructure Hacking

Some Prevalent CVEs of 2020-2022

Table of Contents

Advanced Infrastructure Hacking 0
CVE-2024-36401 7
CVE-2024-30103 7
CVE-2024-6387 7
CVE-2024-21683 8
CVE-2024-4040 8
CVE-2024-3400 8
CVE-2024-21887 9
CVE-2024-23897 9
CVE-2024-0204 9
CVE-2024-21762 10
CVE-2024-34102 10
CVE-2024-4577 11
CVE-2024-4367 11
CVE-2024-32962 12
CVE-2024-30080 13
CVE-2024-21007 13
CVE-2023-21746 13
CVE-2023-2868 14
CVE-2023-3519 14
CVE-2023-38831 15
CVE-2023-1671 15
CVE-2023-21716 15
CVE-2023-38646 16
CVE-2023-46604 16
CVE-2023-27372 16
CVE-2023-22527 17
CVE-2023-38408 17

CVE-2023-0669.....18
CVE-2023-20887.....18
CVE-2023-27997.....19
CVE-2023-29336.....19
CVE-2023-26360.....19
CVE-2023-23397.....20
CVE-2023-32233.....20
CVE-2023-2006.....20
CVE-2023-29325.....20
CVE-2023-29357.....21
CVE-2023-35708.....21
CVE-2023-208870.....21
CVE-2023-3269.....21
CVE-2022-26134.....22
CVE-2022-1388.....22
CVE-2022-0609.....22
CVE-2022-41040 & CVE-2022-41082.....23
CVE-2022-26809.....23
CVE-2022-23307.....23
CVE-2022-22965 (Spring4Shell).....23
CVE-2022-21999 (Spool Fool).....24
CVE-2022-21922.....24
CVE-2022-21888.....24
CVE-2022-0847 (Dirty Pipe).....24
CVE-2022-0543.....26
CVE-2022-26826.....26
CVE-2021-44228 (Log4Shell).....26
CVE-2021-44142.....27
CVE-2021-42313.....27
CVE-2021-42298.....27
CVE-2021–42287.....28

CVE-2021-36934 (SeriousSAM) 28
CVE-2021-24527 28
CVE-2021-1675 (PrintNightmare) 28
CVE-2020-0796 (SMBGhost/Coronablue) 29
CVE-2021-26855 (ProxyLogon) 29
CVE-2020-5902 30
CVE-2020-1472 (Zerologon) 30
CVE-2020-0601 (CurveBall) 30
CVE-2020-1938 (GhostCat) 31
CVE-2020-16898 (Bad Neighbor) 31
CVE-2020-1350 (aka SIGRed) 31
CVE-2021-1732 31
CVE-2020-3452 32
CVE-2021-28480/81 32
CVE-2021-28482 32
CVE-2020-16875 33
CVE-2020-0688 33
CVE-2020-16952 33
CVE-2021-31956 34
CVE-2021-27070 34
CVE-2021-24090 34
CVE-2021-1706 34
CVE-2021-1701 34
CVE-2021-1700 34
CVE-2021-1668 35
CVE-2021-1667 35
CVE-2020-17096 35
CVE-2020-17095 35
CVE-2020-17042 35
CVE-2020-16968 35
CVE-2020-16967 36

CVE-2020-16924.....36
CVE-2020-16911.....36
CVE-2020-1564.....36
CVE-2020-1562.....36
CVE-2020-1561.....36
CVE-2020-1558.....36
CVE-2020-1557.....37
CVE-2020-1508.....37
CVE-2020-1435.....37
CVE-2020-1421.....37
CVE-2020-1416.....37
CVE-2020-1412.....37
CVE-2020-1410.....38
CVE-2020-1409.....38
CVE-2020-1408.....38
CVE-2020-1407.....38
CVE-2020-1401.....38
CVE-2020-1400.....38
CVE-2020-1377.....38
CVE-2020-1319.....39
CVE-2020-1317.....39
CVE-2020-1307.....39
CVE-2020-1299.....39
CVE-2020-1286.....39
CVE-2020-1285.....39
CVE-2020-1248.....40
CVE-2020-1236.....40
CVE-2020-1208.....40
CVE-2020-1176.....40
CVE-2020-1175.....40
CVE-2020-1174.....40

CVE-2020-1153.....40
CVE-2020-1136.....41
CVE-2020-1113.....42
CVE-2020-1112.....42
CVE-2020-1074.....42
CVE-2020-1067.....42
CVE-2020-1061.....42
CVE-2020-1054.....42
CVE-2020-1048.....43
CVE-2020-1039.....43
CVE-2020-1013.....43
CVE-2020-0997.....43
CVE-2021-24094.....43
CVE-2021-24074.....44
CVE-2021-1733.....44
CVE-2020-0646.....44
CVE-2020-0668.....44
CVE-2020-0683.....44
CVE-2020-0787.....44
CVE-2020-0796.....45
CVE-2020-0863.....45
CVE-2020-0932.....45
CVE-2020-0984.....45
CVE-2020-1181.....45
CVE-2020-2551.....45
CVE-2020-3452.....46
CVE-2020-5902.....46
CVE-2020-9484.....46
CVE-2020-14883.....46
CVE-2020-14882.....47
CVE-2020-14859.....47

CVE-2020-13936.....47

CVE-2024-6387

A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead to sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set period.

References:

- https://www.qualys.com/regresshion-cve-2024-6387/

CVE-2024-36401

GeoServer is an open-source server that allows users to share and edit geospatial data. Prior to versions 2.23.6, 2.24.4, and 2.25.2, multiple OGC request parameters allow Remote Code Execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating property names as XPath expressions. The GeoTools library API that GeoServer calls evaluates property/attribute names for feature types in a way that unsafely passes them to the commons-jxpath library which can execute arbitrary code when evaluating XPath expressions. This XPath evaluation is intended to be used only by complex feature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types as well which makes this vulnerability apply to **ALL** GeoServer instances.

References:

- https://github.com/vulhub/vulhub/tree/master/geoserver/CVE-2024-36401
- https://nvd.nist.gov/vuln/detail/CVE-2024-36401

CVE-2024-30103

A critical security vulnerability, identified as CVE-2024-30103, has been discovered in Microsoft Outlook. This flaw is exceptionally dangerous because it is a zero-click remote code execution (RCE) vulnerability. This means that attackers can gain control of your system merely by sending an email—no interaction, such as clicking on links or opening attachments, is required. Just receiving the email can trigger the attack, allowing the attacker to execute commands, install malware, or take over the affected system.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2024-30103

CVE-2024-21683

This High severity RCE (Remote Code Execution) vulnerability was introduced in version 5.2 of Confluence Data Center and Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.2, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2024-21683

CVE-2024-4040

A server-side template injection vulnerability in CrushFTP in all versions before 10.7.1 and 11.1.0 on all platforms allows unauthenticated remote attackers to read files from the filesystem outside of the VFS Sandbox, bypass authentication to gain administrative access, and perform remote code execution on the server.

References:

- https://blog.qualys.com/vulnerabilities-threat-research/2024/04/30/crushftp-zero-day-exploitation-due-to-cve-2024-4040

CVE-2024-3400

A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.

References:

- https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/#RespondingToCompromise

CVE-2024-21887

A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2024-21887
- https://github.com/Chocapikk/CVE-2024-21887

CVE-2024-23897

Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2024-23897
- https://www.splunk.com/en_us/blog/security/security-insights-jenkins-cve-2024-23897-rce.html

CVE-2024-0204

Authentication bypass in Fortra's GoAnywhere MFT prior to 7.4.1 allows an unauthorized user to create an admin user via the administration portal.

References:

- https://nvd.nist.gov/vuln/detail/cve-2024-0204
- https://www.horizon3.ai/attack-research/attack-blogs/cve-2024-0204-fortra-goanywhere-mft-authentication-bypass-deep-dive/

CVE-2024-21762

An out-of-bounds write in Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to execute unauthorized code or commands via specifically crafted requests

References:

- https://nvd.nist.gov/vuln/detail/CVE-2024-21762
- https://www.assetnote.io/resources/research/two-bytes-is-plenty-fortigate-rce-with-cve-2024-21762

CVE-2024-34102

Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by sending a crafted XML document that references external entities. Exploitation of this issue does not require user interaction.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2024-34102
- https://www.vicarius.io/vsociety/posts/cosmicsting-critical-unauthenticated-xxe-vulnerability-in-adobe-commerce-and-magento-cve-2024-34102-exploit

CVE-2024-4577

In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behaviour to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2024-4577
- https://blog.orange.tw/2024/06/cve-2024-4577-yet-another-php-rce.html

CVE-2024-4367

A type check was missing when handling fonts in PDF.js, which would allow arbitrary JavaScript execution in the PDF.js context. This vulnerability affects Firefox < 126, Firefox ESR < 115.11, and Thunderbird < 115.11.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2024-4367
- https://codeanlabs.com/blog/research/cve-2024-4367-arbitrary-js-execution-in-pdf-js/

CVE-2024-32962

xml-crypto is an xml digital signature and encryption library for Node.js. In affected versions the default configuration does not check authorization of the signer, it only checks the validity of the signature per section 3.2.2 of the w3 xmldsig-core-20080610 spec. As such, without additional validation steps, the default configuration allows a malicious actor to re-sign an XML document, place the certificate in a `<KeyInfo />` element, and pass `xml-crypto` default validation checks. As a result, `xml-crypto` trusts by default any certificate provided via digitally signed XML document's `<KeyInfo />`. `xml-crypto` prefers to use any certificate provided via digitally signed XML document's `<KeyInfo />` even if library was configured to use specific certificate (`publicCert`) for signature verification purposes. An attacker can spoof signature verification by modifying XML document and replacing existing signature with signature generated with malicious private key (created by attacker) and by attaching that private key's certificate to `<KeyInfo />` element. This vulnerability is combination of changes introduced to `4.0.0` on pull request 301 / commit `c2b83f98` and has been addressed in version 6.0.0 with pull request 445 / commit `21201723d`. Users are advised to upgrade. Users unable to upgrade may either check the certificate extracted via `getCertFromKeyInfo` against trusted certificates before accepting the results of the validation or set `xml-crypto's getCertFromKeyInfo` to `() => undefined` forcing `xml-crypto` to use an explicitly configured `publicCert` or `privateKey` for signature verification.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2024-32962
- https://securityonline.info/cve-2024-32962-cvss-10-critical-vulnerability-in-xml-crypto-affects-millions/

CVE-2024-30080

In the Message Queuing (MSMQ) vulnerability by sending specially crafted malicious MSMQ packets to the vulnerable servers and thus exploiting the vulnerability, the attackers might achieve remote code execution and take over the unpatched server.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2024-30080

CVE-2024-21007

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2024-21007
- https://www.recordedfuture.com/vulnerability-database/CVE-2024-21007

CVE-2023-21746

The LocalPotato exploit, CVE-2023-21746, presents a significant risk by enabling unauthorized access to sensitive files with SYSTEM-level privileges on Windows systems.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2023-21746
- https://www.vicarius.io/vsociety/posts/unmasking-the-local-potato-a-thrilling-journey-into-the-cve-2023-21746-windows-vulnerability

CVE-2023-2868

A remote command injection vulnerability exists in the Barracuda Email Security Gateway (appliance form factor only) product effecting versions 5.1.3.001-9.2.0.006. The vulnerability arises out of a failure to comprehensively sanitize the processing of .tar file (tape archives). The vulnerability stems from incomplete input validation of a user supplied .tar file as it pertains to the names of the files contained within the archive. As a consequence, a remote attacker can specifically format these file names in a particular manner that will result in remotely executing a system command through Perl's qx operator with the privileges of the Email Security Gateway product.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2023-2868
- https://cloud.google.com/blog/topics/threat-intelligence/barracuda-esg-exploited-globally

CVE-2023-3519

A critical remote code execution vulnerability has been identified in Citrix ADC. Researchers quickly pinpointed the vulnerability to be most likely present in the NetScaler Packet Parsing Engine (nsppe). Initially, it was believed that the vulnerability was a complex heap-based bug requiring SAML to be enabled for exploitation.

References:

- https://bishopfox.com/blog/analysis-exploitation-cve-2023-3519
- https://nvd.nist.gov/vuln/detail/CVE-2023-3519
- https://www.assetnote.io/resources/research/analysis-of-cve-2023-3519-in-citrix-adc-and-netscaler-gateway

CVE-2023-38831

RARLAB WinRAR before 6.23 allows attackers to execute arbitrary code when a user attempts to view a benign file within a ZIP archive. The issue occurs because a ZIP archive may include a benign file (such as an ordinary .JPG file) and a folder that has the same name as the benign file, and the contents of the folder (which may include executable content) are processed during an attempt to access only the benign file.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2023-38831
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/exploring-winrar-vulnerability-cve-2023-38831/

CVE-2023-1671

A vulnerability was found in Sophos Web Appliance versions older than 4.3.10.4. It has been rated as critical. This pre-authentication command injection vulnerability exists in the warn-proceed handler. An attacker can exploit this flaw to execute arbitrary code on the system.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2023-1671
- https://www.picussecurity.com/resource/blog/cve-2023-1671-sophos-command-injection-vulnerability-exploited-in-the-wild

CVE-2023-21716

A vulnerability was found in Microsoft Word which has been rated as critical. This issue involves a heap corruption vulnerability within the DLL "wwlib.dll" used by Microsoft Word when parsing an RTF file. An attacker can exploit this flaw by crafting a malicious RTF file, potentially leading to arbitrary code execution.

References:

- https://www.netskope.com/blog/cve-2023-21716-microsoft-word-rce-vulnerability
- https://nvd.nist.gov/vuln/detail/CVE-2023-21716

CVE-2023-38646

Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2023-38646
- https://www.assetnote.io/resources/research/chaining-our-way-to-pre-auth-rce-in-metabase-cve-2023-38646

CVE-2023-46604

The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath. Users are recommended to upgrade both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3 which fixes this issue.

References:

- https://www.trendmicro.com/en_in/research/23/k/cve-2023-46604-exploited-by-kinsing.html
- https://nvd.nist.gov/vuln/detail/CVE-2023-46604

CVE-2023-27372

A vulnerability was found in SPIP before version 4.2.1. It has been rated as critical. SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. The fixed versions are 3.2.18, 4.0.10, 4.1.8, and 4.2.1.

References:

- https://www.exploit-db.com/exploits/51536
- https://nvd.nist.gov/vuln/detail/CVE-2023-27372

CVE-2023-22527

A template injection vulnerability on older versions of Confluence Data Center and Server allows an unauthenticated attacker to achieve RCE on an affected instance. Customers using an affected version must take immediate action. Most recent supported versions of Confluence Data Center and Server are not affected by this vulnerability as it was ultimately mitigated during regular version updates.

References:

- https://confluence.atlassian.com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html
- https://github.com/Manh130902/CVE-2023-22527-POC

CVE-2023-38408

The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. This issue exists because of an incomplete fix for CVE-2016-10009.

References:

- https://www.vicarius.io/vsociety/posts/exploring-opensshs-agent-forwarding-rce-cve-2023-38408
- https://nvd.nist.gov/vuln/detail/CVE-2023-38408

CVE-2023-46747

A vulnerability was found in F5 BIG-IP. It has been rated as critical. An undisclosed request may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands.

References:

- https://github.com/W01fh4cker/CVE-2023-46747-RCE
- https://threatprotect.qualys.com/2023/10/27/f5-big-ip-unauthenticated-remote-code-execution-vulnerability-cve-2023-46747/
- https://nvd.nist.gov/vuln/detail/CVE-2023-46747

CVE-2023-0669

A critical vulnerability in Fortra (formerly, HelpSystems) GoAnywhere MFT which is a pre-authentication command injection vulnerability in the License Response Servlet due to deserializing an arbitrary attacker-controlled object. This issue was patched in version 7.1.2.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2023-0669
- https://github.com/0xf4n9x/CVE-2023-0669
- https://www.fortra.com/blog/summary-investigation-related-cve-2023-0669

CVE-2023-20887

A command injection vulnerability was found in VMware Aria Operations for Networks, rated as critical. A malicious actor with network access to VMware Aria Operations for Networks may be able to exploit this vulnerability to perform a command injection attack, resulting in remote code execution.

References:

- https://blogs.juniper.net/en-us/threat-research/cve-2023-20887-vmware-aria-operations-for-networks-unauthenticated-remote-code-execution
- https://github.com/sinsinology/CVE-2023-20887

CVE-2023-27997

A critical vulnerability in FortiOS which is OS' of the Fortigate firewalls which lead to remote code execution. This vulnerability is exploited using heap buffer overflow in the OS. There were around 3 lakhs+ of Fortigate SSL VPN devices exposed public.

References:

- https://www.rapid7.com/blog/post/2023/06/12/etr-cve-2023-27997-critical-fortinet-fortigate-remote-code-execution-vulnerability/
- https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign

CVE-2023-29336

A privilege escalation vulnerability rated 7.8 severity was identified in the Win32k, a kernel mode driver. On a successful exploitation, an attacker gain SYSTEM privilege. This vulnerability is relied on the kernel handle address in heap memory.

References:

- https://www.numencyber.com/cve-2023-29336-win32k-analysis
- https://nvd.nist.gov/vuln/detail/CVE-2023-29336

CVE-2023-26360

An improper access control vulnerability in the Adobe ColdFusion would allow an attacker to execute arbitrary code on the system. The method ColdFusion uses to deserialize the untrusted data of the users would cause the vulnerability. The code execution is achieved using sending the specially crafted request.

Reference:

- https://www.bleepingcomputer.com/news/security/cisa-warns-of-adobe-coldfusion-bug-exploited-as-a-zero-day/
- https://nvd.nist.gov/vuln/detail/CVE-2023-26360

CVE-2023-23397

A critical vulnerability in the Microsoft Outlook which requires no user interaction and affected locally installed Outlook. It can be exploited by sending specially crafted email to victims, which doesn't need to be opened. The attackers capture the NTLMv2 hashes by doing this.

Reference:

- https://nvd.nist.gov/vuln/detail/cve-2023-23397
- https://www.balbix.com/blog/urgent-action-recommended-microsoft-outlook-vulnerability-cve-2023-23397/

CVE-2023-32233

A use after free vulnerability identified in the Linux kernel versions 6.3.1 and earlier's netfilter subsystem in net/netfilter/nf_tables_api.c caused by incorrect error path handling. By exploiting this an attacker with user level access can escalate their privileges.

Reference:

- https://nvd.nist.gov/vuln/detail/CVE-2023-3390
- https://ubuntu.com/security/CVE-2023-3390

CVE-2023-2006

A vulnerability in the Linux kernel's RxRPC network protocol can lead an attacker with low prilvilege user access to escalate the privilege. The issue caused due to lack of proper locking while performing operations on the objects.

Reference:

- https://security-tracker.debian.org/tracker/CVE-2023-2006
- https://bugzilla.redhat.com/show_bug.cgi?id=2189112

CVE-2023-29325

A windows OLE remote code execution vulnerability can be achieved by sending the victim a specially crafted email. On victim opening the email could lead to the code execution.

Reference:

- https://www.cvedetails.com/cve/CVE-2023-29325/

CVE-2023-29357

A privilege escalation vulnerability in Microsoft Share Point Server rated 9.8 severity. This attack involves in spoofing the JWT token and crafting it to execute an attack that bypasses the authentication and gain the administrator privilege.

Reference:

- https://nvd.nist.gov/vuln/detail/CVE-2023-29357
- https://vuldb.com/?id.231394

CVE-2023-35708

MOVEit is a tool used for transfer of files across devices and servers. By sending the crafted payload to a MOVEit application endpoint which could result in escalation of privileges and unauthorized access.

Reference:

- https://nvd.nist.gov/vuln/detail/CVE-2023-35708
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-35708

CVE-2023-208870

A vulnerability with severity rated 9.8, would allow an attacker to execute remote code execution on the VMWare Aria Operation for Networks. An unauthenticated users can exploit it without user interaction.

Reference:

- https://www.vmware.com/security/advisories/VMSA-2023-0012.html
- https://nvd.nist.gov/vuln/detail/CVE-2023-20887

CVE-2023-3269

A vulnerability also named as StackRot which impacts Linux versions 6.1 to 6.4. This is a linux kernel vulnerability identified in the memore management subsystem. Also, requires minimum effort to exploit it to gain elevated privileges.

Reference:

- https://access.redhat.com/security/cve/cve-2023-3269

CVE-2022-26134

A critical vulnerability with the rating of 9.8 found in the Atlassian's Confluence, a collaboration tool.

Unauthenticated remote code execution can be achieved by sending specially crafted HTTP request containing OGNL (Object-Graph Navigation Language) in the URI. The attackers using this vulnerability for spreading malware and cryptocurrency mining.

Reference:

- https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26134

CVE-2022-1388

A vulnerability in the F5 BIG IP iControl Rest, a web-based management interface for the BIG IP devices could allow attacker to gain full control of the device by executing the arbitrary code. An attacker could send the specially crafted HTTP request to exploit the vulnerability. The remote code execution vulnerability rated 9.8 severity.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2022-1388
- https://my.f5.com/manage/s/article/K23605346

CVE-2022-0609

Follina (CVE-2022-0609) is a Microsoft Office's high severity vulnerability that hackers can leverage for Remote Code Execution. The vulnerability was exploited by specially crafted Word or RTF file which triggers MSDT (A windows diagnostic tool) to download and execute malicious code. This was used by attackers in phishing also in malwares.

References:

- https://nvd.nist.gov/vuln/detail/cve-2022-30190
- https://logrhythm.com/blog/detecting-follina-cve-2022-30190-microsoft-office-zero-day-exploit

CVE-2022-41040 & CVE-2022-41082

A vulnerability named OWASSRF on the Microsoft exchange servers exploited. A server-side request forgery attack CVE-2022-41040 using which can gain remote code execution if authenticated.

References:

- https://www.crowdstrike.com/blog/owassrf-exploit-analysis-and-recommendations/
- https://nvd.nist.gov/vuln/detail/cve-2022-41082

CVE-2022-26809

CVE-2021-44142 is a vulnerability that allows remote attackers to execute arbitrary code. An integer overflow in MSRPC that, if exploited, allows for arbitrary code execution over the network without requiring authentication or user interaction.

References:

- https://isc.sans.edu/forums/diary/An+Update+on+CVE202226809+MSRPC+Vulnerabliity+PATCH+NOW/28550/
- https://github.com/XmasSnow1/cve-2022-26809

CVE-2022-23307

An attacker may be able to use this vulnerability to generate a Log4j configuration that allows them to perform unauthorized actions. CVE-2020-9493 identified a deserialization issue that was present in Apache Chainsaw. Prior to Chainsaw V2.0 Chainsaw was a component of Apache Log4j 1.2.x where the same issue exists.

References:

- https://support.f5.com/csp/article/K00322972

CVE-2022-22965 (Spring4Shell)

Spring by VMWare has released Spring Cloud Function versions 3.1.7 and 3.2.3 to address remote code execution (RCE) vulnerability CVE-2022-22963 as well as Spring Framework versions 5.3.18 and 5.2.20 to address RCE vulnerability CVE-2022-22965, known as “Spring4Shell.” A remote attacker could exploit these vulnerabilities to take control of an affected system.

References:

- https://www.contrastsecurity.com/security-influencers/new-spring4shell-vulnerability-confirmed-what-it-is-and-how-to-be-prepared

- https://github.com/FourCoreLabs/spring4shell-exploit-poc

CVE-2022-21999 (Spool Fool)

CVE-2022-21999 known as SpoolFool is a local privilege escalation vulnerability found in the print spooler service of Microsoft Windows, which manages print processes. The SpoolFool vulnerability bypasses security checks present in earlier print spool privilege escalation vulnerabilities by manipulating the path of a printer port such that it's possible to create directories in the printer spool driver directory and load arbitrary DLL files from it and execute with administrative privileges.

References:

- https://www.secplicity.org/2022/02/23/spoolfool-windows-print-spooler-fooled-again/
- https://github.com/ly4k/SpoolFool

CVE-2022-21922

A vulnerability was found in Microsoft Windows (Operating System). It has been rated as critical. Affected by this issue is an unknown functionality of the component Remote Procedure Call Runtime. Confidentiality, integrity, and availability is impacted by the exploit.

References:

- https://vuldb.com/?id.190142

CVE-2022-21888

The vulnerability allows a remote attacker to execute arbitrary code on the target system. The vulnerability exists due to improper input validation in Windows Modern Execution Server. A remote attacker can send a specially crafted request and execute arbitrary code on the target system. Successful exploitation of this vulnerability may result in complete compromise of vulnerable system.

References:

- https://www.cybersecurity-help.cz/vdb/SB2022011129
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21888

CVE-2022-0847 (Dirty Pipe)

A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in ‘copy_page_to_iter_pipe’ and 'push_pipe’ functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system.

References:

- https://dirtypipe.cm4all.com/
- https://github.com/0xIronGoat/dirty-pipe

CVE-2022-0543

Reginaldo Silva discovered that due to a packaging issue, a remote attacker with the ability to execute arbitrary Lua scripts could possibly escape the Lua sandbox and execute arbitrary code on the host.

References:

- https://github.com/aodsec/CVE-2022-0543

CVE-2022-26826

CVE-2022-26826 is a Remote Code Execution (RCE) vulnerability, present on Windows DNS Server.

References:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26826

CVE-2021-44228 (Log4Shell)

CVE-2021-44228 a Remote Code Execution (RCE) vulnerability in Apache's Log4j functionality. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

References:

- https://nakedsecurity.sophos.com/2021/12/13/log4shell-explained-how-it-works-why-you-need-to-know-and-how-to-fix-it/
- https://github.com/pentesterland/Log4Shell

CVE-2021-44142

CVE-2021-44142 is a vulnerability that allows remote attackers to execute arbitrary code on affected installations of Samba. The specific gap exists in the parsing of the EA metadata in the server daemon smbd when opening a file. An attacker can abuse this vulnerability to execute code in the root context even without authentication.

References:

- https://www.trendmicro.com/en_ae/research/22/b/the-samba-vulnerability-what-is-cve-2021-44142-and-how-to-fix-it.html
- https://gist.github.com/0xsha/0859033e1777490576923a27fbcd23ac

CVE-2021-42313

This vulnerability allows remote attackers to bypass authentication on affected installations of Microsoft Azure Defender for IoT. Authentication is not required to exploit this vulnerability. The specific flaw exists within the sync endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to bypass authentication on the system and execute arbitrary code in the context of root.

References:

- https://www.zerodayinitiative.com/advisories/ZDI-21-1555/

CVE-2021-42298

CVE-2021-42298 a Remote Code Execution (RCE) vulnerability in Microsoft Defender. The vulnerability exists due to improper input validation in Microsoft Defender. A remote attacker can execute arbitrary code on the target system.

References:

- https://www.cybersecurity-help.cz/vdb/SB2021110921
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42298

CVE-2021–42287

CVE-2021–42278 and CVE-2021–42287 allow an adversary with access to low-privileged domain user credentials, to obtain a Kerberos Service Ticket for a Domain Controller computer account. This effectively allows a regular domain user to take control of a domain controller.

References:

- https://medium.com/@mvelazco/hunting-for-samaccountname-spoofing-cve-2021-42287-and-domain-controller-impersonation-f704513c8a45
- https://github.com/WazeHell/sam-the-admin

CVE-2021-36934 (SeriousSAM)

Since Windows 10 build 1809, the Access Control Lists (ACLs) for '%windir%\System32\config' have been granting read access to non-admin users. This is the primary directory that contains the files for the Windows Registry, including the Security Account Manager (SAM) which stores users' passwords. An attacker with the ability to execute code on a target host could exploit this vulnerability to elevate their privileges to SYSTEM.

References:

- https://news.sophos.com/en-us/2021/07/22/hivenightmare-aka-serioussam-vulnerability-what-to-do/
- https://github.com/romarroca/SeriousSam

CVE-2021-24527

CVE-2021-24527 is an account takeover vulnerability. The User Registration & User Profile Builder WordPress plugin before 3.4.9 has a bug allowing any user to reset the password of the admin of the blog, and gain unauthorised access, due to a bypass in the way the reset key is checked. Furthermore, the admin will not be notified of such change by email

References:

- https://wpscan.com/vulnerability/c142e738-bc4b-4058-a03e-1be6fca47207

CVE-2021-1675 (PrintNightmare)

CVE-2021-1675 is a remote code execution in Windows Print Spooler. According to the MSRC security bulletin, this vulnerability is reported by Zhipeng Huo, Piotr Madej and Zhang Yunhai. This vulnerability can be used to achieve LPE and RCE. As for the RCE part, you need a user to authenticate on the Spooler service. However, this is still critical in the Domain environment.

Because normally DC will have Spooler service enabled, a compromised domain user may use this vulnerability to control the DC.

References:

- https://github.com/calebstewart/CVE-2021-1675
- https://github.com/rapid7/metasploit-framework/pull/15385
- https://github.com/cube0x0/CVE-2021-1675

CVE-2020-0796 (SMBGhost/Coronablue)

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.

References:

- https://blog.zecops.com/research/vulnerability-reproduction-cve-2020-0796-poc/
- https://blog.zecops.com/research/smbleedingghost-writeup-chaining-smbleed-cve-2020-1206-with-smbghost/

CVE-2021-26855 (ProxyLogon)

Microsoft Exchange ProxyLogon RCE which allows unauthenticated remote code execution on Microsoft Exchange. Exploitation requires knowledge of the frontend Exchange server URL (e.g., https://exchange.example.org) and an email address for a user on the system. The admin SID and backend can be leaked from the server.

References:

- https://www.rapid7.com/db/modules/exploit/windows/http/exchange_proxylogon_rce/
- https://github.com/praetorian-inc/proxylogon-exploit

CVE-2020-5902

In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.

References:

- https://github.com/yasserjanah/CVE-2020-5902

CVE-2020-1472 (Zerologon)

CVE-2020-1472 is a privilege escalation vulnerability due to the insecure usage of AES-CFB8 encryption for Netlogon sessions. The AES-CFB8 standard requires that each byte of plaintext, like a password, must have a randomized initialization vector (IV) so that passwords cannot be guessed. The ComputeNetlogonCredential function in Netlogon sets the IV to a fixed 16 bits, which means an attacker could control the deciphered text. An attacker can exploit this flaw to impersonate the identity of any machine on a network when attempting to authenticate to the Domain Controller (DC).

Reference

- https://github.com/SecuraBV/CVE-2020-1472
- https://www.secura.com/blog/zero-logon

CVE-2020-0601 (CurveBall)

A code-level root cause analysis of CVE-2020-0601 in the context of how applications are likely to use CryptoAPI to handle certificates — more specifically in the context of applications communicating via Transport Layer Security (TLS).

References:

- https://www.trendmicro.com/en_us/research/20/b/an-in-depth-technical-analysis-of-curveball-cve-2020-0601.html

CVE-2020-1938 (GhostCat)

CVE-2020-1938 is a file read/inclusion vulnerability in the AJP connector in Apache Tomcat. This is enabled by default with a default configuration port of 8009. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious Java Server Pages (JSP) code within a variety of file types and trigger this vulnerability to gain remote code execution (RCE).

References:

- https://www.chaitin.cn/en/ghostcat

CVE-2020-16898 (Bad Neighbor)

A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets that use Option Type 25 (Recursive DNS Server Option) and a length field value that is even.

References:

- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/bad-neighbors-can-break-windows-cve-2020-16898/

CVE-2020-1350 (aka SIGRed)

This is a critical wormable RCE vulnerability in a Windows DNS Server, which can affect all Windows server versions and can be triggered by a malicious DNS response. Adversaries only need to send a specially generated request to the DNS server to run malicious code in the context of the LocalSystem account (a predefined local account used by the service control manager). The LocalSystem account is not recognized by the security subsystem, and according to Microsoft, the main danger of the vulnerability is that it can be used to spread a threat over a local network.

CVE-2021-1732

It exists in the Windows Win32k operating system kernel and is an elevation-of-privilege (EoP) vulnerability. It would allow a logged-on user to execute code of their choosing with higher privileges, by running a specially crafted application. If successful, attackers could execute code in the context of the kernel and gain SYSTEM privileges, essentially giving the attacker free rein to do whatever they wanted on the compromised machine.

References:

- https://github.com/KaLendsi/CVE-2021-1732-Exploit

CVE-2020-3452

A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system.

References:

- https://github.com/PR3R00T/CVE-2020-3452-Cisco-Scanner

CVE-2021-28480/81

Microsoft Exchange Server Remote Code Execution Vulnerability (pre-authentication). CVE-2021-28480 and CVE-2021-28481 are pre-authentication vulnerabilities in Microsoft Exchange Server. A pre-authentication vulnerability means that an attacker does not need to authenticate to the vulnerable Exchange Server to exploit the vulnerability. All the attacker needs to do is perform reconnaissance against their intended targets and then send specially crafted requests to the vulnerable Exchange Server.

References:

- https://www.tenable.com/blog/cve-2021-28480-cve-2021-28481-cve-2021-28482-cve-2021-28483-four-critical-microsoft-exchange

CVE-2021-28482

Microsoft Exchange Server Remote Code Execution Vulnerability (Post-authentication). Attackers can exploit this deserialization vulnerability if they are authenticated on an on-premises Exchange Server instance.

References:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-28482
- https://gist.github.com/testanull/9ebbd6830f7a501e35e67f2fcaa57bda
- https://www.bleepingcomputer.com/news/security/poc-exploit-released-for-microsoft-exchange-bug-discovered-by-nsa/

CVE-2020-16875

A remote code execution vulnerability exists in Microsoft Exchange server due to improper validation of cmdlet arguments. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the System user, aka 'Microsoft Exchange Server Remote Code Execution Vulnerability.

References:

- https://www.rapid7.com/db/vulnerabilities/msft-cve-2020-16875/
- https://packetstormsecurity.com/files/159210/Microsoft-Exchange-Server-DlpUtils-AddTenantDlpPolicy-Remote-Code-Execution.html
- https://srcincite.io/pocs/cve-2020-16875.py.txt
- https://srcincite.io/pocs/cve-2020-16875.ps1.txt

CVE-2020-0688

Microsoft Exchange default MachineKeySection deserialize vulnerability. The CVE-2020-0688 vulnerability affects the Exchange Control Panel (ECP) component. The vulnerability affects all installations of Exchange Server because until the most recent patch, all Exchange Servers had the same validation key and validation algorithm in the web.config file. The POC exploits take advantage of same validation key and validation algorithm to craft a serialized __VIEWSTATE request parameter containing an embedded command, signed with the valid key.

References:

- https://github.com/zcgonvh/CVE-2020-0688
- https://www.exploit-db.com/exploits/48153
- https://www.trustedsec.com/blog/detecting-cve-20200688-remote-code-execution-vulnerability-on-microsoft-exchange-server/

CVE-2020-16952

A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint.

References:

- https://www.rapid7.com/db/vulnerabilities/msft-cve-2020-16952/

CVE-2021-31956

CVEAn EoP vulnerability within Windows NTFS (New Technology File System) which could allow a local user to elevate their privileges on an affected system. A local user could exploit the flaw with a crafted application to take control of a system. This vulnerability affects all currently supported Windows variants including Windows Server and Windows Server Core Installations.

CVE-2021-27070

Windows 10 Update Assistant Elevation of Privilege Vulnerability. The specific flaw exists within the Windows Update Assistant. The issue results from incorrect permissions on a directory. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of Administrator. This vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.

CVE-2021-24090

Windows Error Reporting Elevation of Privilege Vulnerability. The vulnerability exists due to application does not properly impose security restrictions in Windows Error Reporting, which leads to security restrictions bypass and privilege escalation. The vulnerability allows a local attacker to escalate privileges on the system.

CVE-2021-1706

Windows LUAFV Elevation of Privilege Vulnerability. The vulnerability exists due to application does not properly impose security restrictions in Windows LUAFV, which leads to security restrictions bypass and privilege escalation. The vulnerability allows a local user to escalate privileges on the system.

CVE-2021-1701

The vulnerability allows a remote attacker to execute arbitrary code on the system. The vulnerability exists due to insufficient validation of user-supplied input in Remote Procedure Call Runtime. A remote authenticated attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

CVE-2021-1700

The vulnerability allows a remote attacker to execute arbitrary code on the system. The vulnerability exists due to insufficient validation of user-supplied input in Remote Procedure Call Runtime. A

remote authenticated attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

CVE-2021-1668

The vulnerability allows a remote attacker to execute arbitrary code on the system. The vulnerability exists due to insufficient validation of user-supplied input in Microsoft DTV-DVD Video Decoder. A remote attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

CVE-2021-1667

The vulnerability exists due to insufficient validation of user-supplied input in Remote Procedure Call Runtime. A remote authenticated attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

CVE-2020-17096

The vulnerability exists due to insufficient validation of user-supplied input in Windows NTFS. A remote authenticated attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

CVE-2020-17095

The vulnerability exists due to insufficient validation of user-supplied input in Hyper-V. A remote authenticated attacker can pass specially crafted input to the application and execute arbitrary code on the target system.

CVE-2020-17042

The vulnerability exists due to improper input validation in Windows Print Spooler. A remote attacker can send a specially crafted request and execute arbitrary code on the target system. Successful exploitation of this vulnerability may result in complete compromise of the vulnerable system.

CVE-2020-16968

The vulnerability exists due to a boundary error within the Windows Camera Codec Pack. A remote attacker can create a specially crafted file, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system. Successful exploitation of this vulnerability may result in complete compromise of the vulnerable system.

CVE-2020-16967

The vulnerability exists due to a boundary error within the Windows Camera Codec Pack. A remote attacker can create a specially crafted file, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

CVE-2020-16924

The vulnerability exists due to a boundary error within the Windows Jet Database Engine. A remote attacker can create a specially crafted file, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

CVE-2020-16911

The vulnerability exists due to the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory. A local user can use a specially crafted application, trigger out-of-bounds read error and read contents of memory on the system.

CVE-2020-1564

The vulnerability exists due to a boundary error within the Windows Jet Database Engine. A remote attacker can create a specially crafted file, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

CVE-2020-1562

The vulnerability exists due to a boundary error within Microsoft Graphics Components when processing TTF fonts in fontdrvhost. A remote attacker can create a specially crafted webpage, trick the victim into opening it, trigger use-after-free error and execute arbitrary code on the target system.

CVE-2020-1561

The vulnerability exists due to a boundary error within Microsoft Graphics Components when processing TTF fonts in fontdrvhost. A remote attacker can create a specially crafted webpage, trick the victim into opening it, trigger use-after-free error and execute arbitrary code on the target system.

CVE-2020-1558

The vulnerability exists due to a boundary error within the Windows Jet Database Engine. A remote attacker can create a specially crafted file, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

CVE-2020-1557

The vulnerability exists due to a boundary error within the Windows Jet Database Engine. A remote attacker can create a specially crafted file, trick the victim into opening it, trigger memory corruption and execute arbitrary code on the target system.

CVE-2020-1508

The vulnerability exists due to a boundary error when Windows Media Audio Decoder improperly handles objects. A remote authenticated attacker can trick a victim to open a specially crafted document or visit a malicious webpage, trigger memory corruption, and execute arbitrary code on the target system.

CVE-2020-1435

The vulnerability exists due to a boundary error when Windows Graphics Device Interface (GDI) handles objects in the memory. A remote attacker can trick a victim to open a specially crafted file or visit a malicious website, trigger memory corruption, and execute arbitrary code on the target system.

CVE-2020-1421

The vulnerability exists due to insufficient validation of user-supplied input in Microsoft Windows. A remote attacker can present to the user a removable drive, or remote share, that contains a malicious .LNK file and execute arbitrary code on the target system.

CVE-2020-1416

The vulnerability exists due to application does not properly impose security restrictions in Visual Studio and Visual Studio Code when they load software dependencies. A local user can plant malicious content on an affected computer and wait for another user to launch Visual Studio or Visual Studio Code, leading to privilege escalation.

CVE-2020-1412

A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'.

CVE-2020-1410

A remote code execution vulnerability exists when Windows Address Book (WAB) improperly processes vCard files. To exploit the vulnerability, an attacker could send a malicious vCard that a victim opens using Windows Address Book (WAB), aka 'Windows Address Book Remote Code Execution Vulnerability'.

CVE-2020-1409

A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'.

CVE-2020-1408

A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'.

CVE-2020-1407

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1400, CVE-2020-1401.

CVE-2020-1401

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1400, CVE-2020-1407.

CVE-2020-1400

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1401, CVE-2020-1407.

CVE-2020-1377

An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. An attacker who successfully exploited the vulnerability could gain elevated privileges on a targeted system. A locally authenticated attacker could exploit this vulnerability by running a specially crafted application. The security update addresses the vulnerability by helping to ensure that the Windows Kernel API properly handles objects in memory.

References:

- https://www.rapid7.com/db/vulnerabilities/msft-cve-2020-1377/
- https://github.com/sailay1996/cve-2020-1337-poc

CVE-2020-1319

A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1129.

CVE-2020-1317

An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'.

CVE-2020-1307

An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0986, CVE-2020-1237, CVE-2020-1246, CVE-2020-1262, CVE-2020-1264, CVE-2020-1266, CVE-2020-1269, CVE-2020-1273, CVE-2020-1274, CVE-2020-1275, CVE-2020-1276, CVE-2020-1316.

CVE-2020-1299

A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.

CVE-2020-1286

A remote code execution vulnerability exists when the Windows Shell does not properly validate file paths. An attacker who successfully exploited this vulnerability could run arbitrary code in the context of the current user, aka 'Windows Shell Remote Code Execution Vulnerability'.

CVE-2020-1285

A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'.

CVE-2020-1248

A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'.

CVE-2020-1236

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1208.

CVE-2020-1208

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1236.

CVE-2020-1176

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1175.

CVE-2020-1175

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1176.

CVE-2020-1174

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1175, CVE-2020-1176.

CVE-2020-1153

A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'.

CVE-2020-1136

A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1126, CVE-2020-1150.

CVE-2020-1113

A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'.

CVE-2020-1112

An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'.

CVE-2020-1074

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1039.

CVE-2020-1067

A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'.

CVE-2020-1061

A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory, aka 'Microsoft Script Runtime Remote Code Execution Vulnerability'.

CVE-2020-1054

An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory.

References:

- https://www.cvedetails.com/cve/CVE-2020-1054/
- https://www.rapid7.com/db/vulnerabilities/msft-cve-2020-1054/

.

CVE-2020-1048

An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted script or application. The update addresses the vulnerability by correcting how the Windows Print Spooler Component writes to the file system.

References:

- https://www.rapid7.com/db/vulnerabilities/msft-cve-2020-1048/
- https://github.com/shubham0d/CVE-2020-1048

CVE-2020-1039

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1074.

CVE-2020-1013

An elevation of privilege vulnerability exists when Microsoft Windows processes group policy updates, aka 'Group Policy Elevation of Privilege Vulnerability'.

CVE-2020-0997

A remote code execution vulnerability exists when the Windows Camera Codec Pack improperly handles objects in memory, aka 'Windows Camera Codec Pack Remote Code Execution Vulnerability'.

CVE-2021-24094

Microsoft Windows TCP/IP Remote Code Execution Vulnerability.

References:

- https://github.com/0vercl0k/CVE-2021-24086

CVE-2021-24074

This vulnerability exists in the IPv4 source routing which is blocked by default in Windows systems. Attackers, via a crafted IP packet, could exploit this vulnerability to execute arbitrary code on a target host. This vulnerability, with a CVSS score of 9.8, affects all versions of Windows. Affected users are advised to apply the updates for protection as soon as possible.

References:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-24074

CVE-2021-1733

A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0609.

CVE-2020-0646

A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly, aka '.NET Framework Remote Code Execution Injection Vulnerability'.

CVE-2020-0668

An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672.

CVE-2020-0683

An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'.

CVE-2020-0787

An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) improperly handles symbolic links, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'.

CVE-2020-0796

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.

CVE-2020-0863

An information vulnerability exists when Windows Connected User Experiences and Telemetry Service improperly discloses file information, aka 'Connected User Experiences and Telemetry Service Information Disclosure Vulnerability'.

CVE-2020-0932

A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0920, CVE-2020-0929, CVE-2020-0931, CVE-2020-0971, CVE-2020-0974.

CVE-2020-0984

An elevation of privilege vulnerability exists when the Microsoft AutoUpdate (MAU) application for Mac improperly validates updates before executing them, aka 'Microsoft (MAU) Office Elevation of Privilege Vulnerability'.

CVE-2020-1181

A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls, aka 'Microsoft SharePoint Server Remote Code Execution Vulnerability'.

CVE-2020-2551

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts).

CVE-2020-3452

A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files.

CVE-2020-5902

In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.

CVE-2020-9484

When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed.

CVE-2020-14883

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts).

CVE-2020-14882

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts).

CVE-2020-14859

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts).

CVE-2020-13936

An attacker that can modify Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running the Servlet container. This applies to applications that allow untrusted users to upload/modify velocity templates running Apache Velocity Engine versions up to 2.2.