Co-Authored by:

TLP:WHITE

Product ID: AA21-209A

July 28, 2021

Top Routinely Exploited Vulnerabilities

SUMMARY

This Joint Cybersecurity Advisory was coauthored by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre (ACSC), the United Kingdom's National Cyber Security Centre (NCSC), and the U.S. Federal Bureau of Investigation (FBI).

This advisory provides details on the top 30 vulnerabilities—primarily Common Vulnerabilities and Exposures (CVEs)—routinely exploited by malicious cyber actors in 2020 and those being widely exploited thus far in 2021[1].

Cyber actors continue to exploit publicly known—and often dated—software vulnerabilities against broad target sets, including public and private sector organizations worldwide. However, entities worldwide can mitigate the vulnerabilities listed in this report by applying the available patches to their systems and implementing a centralized patch management system.

Key Findings

In 2020, cyber actors readily exploited recently disclosed vulnerabilities to compromise unpatched systems. Based on available data to the U.S. Government, **a majority of the top vulnerabilities targeted in 2020 were disclosed during the past two years**. Cyber actor exploitation of more recently disclosed software flaws in 2020 probably stems, in part, from the expansion of remote work options amid the COVID-19 pandemic. The rapid shift and increased use of remote work options, such as virtual private networks (VPNs) and cloud-based environments, likely placed additional burden on cyber defenders struggling to maintain and keep pace with routine software patching.

Four of the most targeted vulnerabilities in 2020 affected remote work, VPNs, or cloud-based technologies. Many VPN gateway devices remained unpatched during 2020, with the growth of remote work options challenging the ability of organization to conduct rigorous patch management.

1 The CVEs included in this report are those routinely exploited during 2020 based on observed activity by CISA, ACSC, the NCSC, and FBI within their respective purviews.

CISA, ACSC, the NCSC, and FBI consider the vulnerabilities listed in table 1 to be the topmost regularly exploited CVEs by cyber actors during 2020.

Table 1:Top Routinely Exploited CVEs in 2020

Vendor	CVE	Type
Citrix	CVE-2019-19781	arbitrary code execution
Pulse	CVE 2019-11510	arbitrary file reading
Fortinet	CVE 2018-13379	path traversal
F5- Big IP	CVE 2020-5902	remote code execution (RCE)
MobileIron	CVE 2020-15505	RCE
Microsoft	CVE-2017-11882	RCE
Atlassian	CVE-2019-11580	RCE
Drupal	CVE-2018-7600	RCE
Telerik	CVE 2019-18935	RCE
Microsoft	CVE-2019-0604	RCE
Microsoft	CVE-2020-0787	elevation of privilege
Netlogon	CVE-2020-1472	elevation of privilege

In 2021, malicious cyber actors continued to target vulnerabilities in perimeter-type devices. Among those highly exploited in 2021 are vulnerabilities in Microsoft, Pulse, Accellion, VMware, and Fortinet.

CISA, ACSC, the NCSC, and FBI assess that public and private organizations worldwide remain vulnerable to compromise from the exploitation of these CVEs. Malicious cyber actors will most likely continue to use older known vulnerabilities, such as CVE-2017-11882 affecting Microsoft Office, as long as they remain effective and systems remain unpatched. Adversaries' use of known vulnerabilities complicates attribution, reduces costs, and minimizes risk because they are not investing in developing a zero-day exploit for their exclusive use, which they risk losing if it becomes known.

Organizations are encouraged to remediate or mitigate vulnerabilities as quickly as possible to reduce the risk of exploitation. Most can be remediated by patching and updating systems. Organizations that have not remediated these vulnerabilities should investigate for the presence of IOCs and, if compromised, initiate incident response and recovery plans. See the Contact Information section below for how to reach CISA to report an incident or request technical assistance.

TECHNICAL DETAILS

2020 CVEs

CISA, ACSC, the NCSC, and FBI have identified the following as the topmost exploited vulnerabilities by malicious cyber actors from 2020: CVE-2019-19781, CVE-2019-11510, CVE-2018-13379, CVE-2020-5902, CVE-2020-15505, CVE-2020-0688, CVE-2019-3396, CVE-2017-11882, CVE-2019-11580, CVE-2018-7600, CVE 2019-18935, CVE-2019-0604, CVE-2020-0787, CVE-2020-1472.[1][2][3] Among these vulnerabilities, CVE-2019-19781 was the most exploited flaw in 2020, according to U.S. Government technical analysis.CVE-2019-19781 is a recently disclosed critical vulnerability in Citrix's Application Delivery Controller (ADC)—a load balancing application for web, application, and database servers widely use throughout the United States.[4][5] Nation-state and criminal cyber actors most likely favor using this vulnerability because it is easy to exploit, Citrix servers are widespread, and exploitation enables the actors to perform unauthorized RCE on a target system.[6]

Identified as emerging targets in early 2020,[7] unremediated instances of CVE-2019-19781 and CVE-2019-11510 continued to be exploited throughout the year by nation-state advanced persistent threat actors (APTs) who leveraged these and other vulnerabilities, such as CVE-2018-13379[8][9], in VPN services[10][11] to compromise an array of organizations, including those involved in COVID-19 vaccine development.[12][13]

The CVE-2019-11510 vulnerability in Pulse Connect Secure VPN was also frequently targeted by nation-state APTs. Actors can exploit the vulnerability to steal the unencrypted credentials for all users on a compromised Pulse VPN server and retain unauthorized credentials for all users on a compromised Pulse VPN server and can retain unauthorize access after the system is patched unless all compromised credentials are changed. Nation-state APTs also commonly exploited CVE-2020-15505 and CVE-2020-5902.[14][15][16][17]

2021 CVEs

In 2021, cyber actors continued to target vulnerabilities in perimeter-type devices. In addition to the 2020 CVEs listed above, organizations should prioritize patching for the following CVEs known to be exploited.

- **Microsoft Exchange:** CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065
  - See CISA's Alert: Mitigate Microsoft Exchange Server Vulnerabilities for more information on identifying and mitigating malicious activity concerning these vulnerabilities.
- **Pulse Secure:** CVE-2021-22893, CVE-2021-22894, CVE-2021-22899, and CVE-2021-22900
  - See CISA's Alert: Exploitation of Pulse Connect Secure Vulnerabilities for more information on how to investigate and mitigate this malicious activity.
- **Accellion:** CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104
  - See the Australia-New Zealand-Singapore-UK-U.S. Joint Cybersecurity Advisory: Exploitation of Accellion File Transfer Appliance for technical details and mitigations.
- **VMware:** CVE-2021-21985

- See CISA's Current Activity: Unpatched VMware vCenter Software for more information and guidance.

- **Fortinet:** CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591
  - See the CISA-FBI Joint Cybersecurity Advisory: APT Actors Exploit Vulnerabilities to Gain Initial Access for Future Attacks for more details and mitigations.

MITIGATIONS AND INDICATORS OF COMPROMISE

One of the most effective best practices to mitigate many vulnerabilities is to update software versions once patches are available and as soon as is practicable. If this is not possible, consider applying temporary workarounds or other mitigations, if provided by the vendor. If an organization is unable to update all software shortly after a patch is released, prioritize implementing patches for CVEs that are already known to be exploited or that would be accessible to the largest number of potential attackers (such as internet-facing systems). This advisory highlights vulnerabilities that should be considered as part of the prioritization process. To further assist remediation, automatic software updates should be enabled whenever possible.

Focusing scarce cyber defense resources on patching those vulnerabilities that cyber actors most often use offers the potential of bolstering network security while impeding our adversaries' operations. For example, nation-state APTs in 2020 extensively relied on a single RCE vulnerability discovered in the Atlassian Crow, a centralized identity management and application (CVE-2019-11580) in its reported operations. A concerted focus on patching this vulnerability could have a relative broad impact by forcing the actors to find alternatives, which may not have the same broad applicability to their target set.

Additionally, attackers commonly exploit weak authentication processes, particularly in external-facing devices. Organizations should require multi-factor authentication to remotely access networks from external sources, especially for administrator or privileged accounts.

Tables 2–14 provide more details about, and specific mitigations for, each of the top exploited CVEs in 2020.

Note: The lists of associated malware corresponding to each CVE below are not meant to be exhaustive but intended to identify a malware family commonly associated with exploiting the CVE.

Table 2: CVE-2019-19781 Vulnerability Details

Citrix Netscaler Directory Traversal (CVE-2019-19781)	
Vulnerability Description Citrix Netscaler Application Delivery Control (ADC) is vulnerable to RCE and full system compromise due to poor access controls, thus allowing directory traversal.	**CVSS 3.0[2]** Critical
Vulnerability Discussion, IOCs, and Malware Campaigns	**Fix**

[2] The Common Vulnerability Scoring System (CVSS) version 3.0 is used to assign severity to the vulnerabilities listed in this advisory.

The lack of adequate access controls allows an attacker to enumerate system directories for vulnerable code (directory traversal). In this instance, Citrix ADC maintains a vulnerable Perl script (newbm.pl) that, when accessed via HTTP POST request (POST https://$TARGET/vpn/../vpn/portal/scripts/newbm.pl), allows local operating system (OS) commands to execute. Attackers can use this functionality to upload/execute command and control (C2) software (webshell or reverse-shell executable) using embedded commands (e.g., curl, wget, Invoke-WebRequest) and gain unauthorized access to the OS. *Multiple malware campaigns, including NOTROBIN, have taken advantage of this vulnerability.*	Patch Available

Recommended Mitigations

- Implement the appropriate refresh build according to the vulnerability details outlined by the vendor: Citrix: Mitigation Steps for CVE-2019-19781
- If possible, only allow the VPN to communicate with known Internet Protocol (IP) addresses (allow-list).

Detection Methods

- CISA has developed a free detection tool for this vulnerability: cisagov/check-cve-2019-19781: Test a host for susceptibility to CVE-2019-19781.
- Nmap developed a script that can be used with the port scanning engine: CVE-2019-19781 - Citrix ADC Path Traversal #1893.
- Citrix also developed a free tool for detecting compromises of Citrix ADC Appliances related to CVE-2019-19781: Citrix / CVE-2019-19781: IOC Scanner for CVE-2019-19781.
- CVE-2019-19781 is commonly exploited to install web shell malware. The National Security Agency (NSA) provides guidance on detecting and preventing web shell malware at https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF and signatures at https://github.com/nsacyber/Mitigating-Web-Shells.

Vulnerable Technologies and Versions

Citrix ADC and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0

References and Additional Guidance

- Citrix Blog: Citrix releases final fixes for CVE-2019-19781
- National Institute for Standards and Technology (NIST) National Vulnerability Database (NVD): Vulnerability Detail CVE-2019-19781
- Tripwire Vulnerability and Exposure Research Team (VERT) Article: Citrix NetScaler CVE-2019-19781: What You Need to Know
- National Security Agency Cybersecurity Advisory: Critical Vulnerability In Citrix Application Delivery Controller (ADC) And Citrix Gateway
- CISA Alert: Detecting Citrix CVE-2019-19781
- NCSC Alert: Actors Exploiting Citrix Products Vulnerability
- CISA-NCSC Joint Cybersecurity Advisory: COVID-19 Exploited by Malicious Cyber Actors
- CISA Alert: Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANOP
- FBI-CISA Joint Cybersecurity Advisory: Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders
- DoJ: Seven International Cyber Defendants, Including “Apt41” Actors, Charged in Connection with Computer Intrusion Campaigns Against More Than 100 Victims Globally
- FBI News: Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks
- FBI FLASH: Indictment of China-Based Cyber Actors Associated with APT 41 for Intrusion Activities
- GitHub: nsacyber / Mitigating Web Shells

Table 3: CVE 2019-11510 Vulnerability Details

Pulse Secure Connect VPN (CVE 2019-11510)	
Vulnerability Description Pulse Secure Connect is vulnerable to unauthenticated arbitrary file disclosure. An attacker can exploit this vulnerability to gain access to administrative credentials.	**CVSS 3.0** Critical
Vulnerability Discussion, IOCs, and Malware Campaigns Improper access controls allow a directory traversal that an attacker can exploit to read the contents of system files. For example, the attacker could use a string such as https://sslvpn.insecure-org.com/dana-na/../dana/html5/acc/guacmole/../../../../../../etc/passwd?/dana/html5/guacamole/ to obtain the local password file from the system. The attacker can also obtain admin session data and replay session tokens in the browser. Once compromised, an attacker can run arbitrary scripts on any host that connects to the VPN. This could lead to anyone connecting to the VPN as a potential target to compromise. *Multiple malware campaigns have taken advantage of this vulnerability, most notably REvil/Sodinokibi ransomware.*	**Fix** Patch Available
Recommended Mitigations • Upgrade to the latest Pulse Secure VPN. • Stay alert to any scheduled tasks or unknown files/executables. • Create detection/protection mechanisms that respond on directory traversal (/../../../) attempts to read local system files.	
Detection Methods • CISA developed a tool to help determine if IOCs exist in the log files of a Pulse Secure VPN Appliance for CVE-2019-11510: cisagov/check-your-pulse. • Nmap developed a script that can be used with the port scanning engine: http-vuln-cve2019-11510.nse #1708.	
Vulnerable Technologies and Versions Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4 are vulnerable.	
References • NIST NVD Vulnerability Detail: CVE-2019-11510 • CISA Alert: Continued Threat Actor Exploitation Post Pulse Secure VPN Patching • Pulse Security Advisory: SA44101 – 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX • GitHub: cisagov / Check Your Pulse • CISA Analysis Report: Federal Agency Compromised by Malicious Cyber Actor • CISA Alert: Exploitation of Pulse Connect Secure Vulnerabilities • CISA-FBI Joint Cybersecurity Advisory: Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets • NCSC Alert: Vulnerabilities Exploited in VPN Products Used Worldwide • DoJ Press Release: Seven International Cyber Defendants, Including “Apt41” Actors, Charged in Connection with Computer Intrusion Campaigns Against More Than 100 Victims Globally • FBI News: Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks • FBI FLASH: Indicators Associated with Netwalker Ransomware • FBI FLASH: Indictment of China-Based Cyber Actors Associated with APT 41 for Intrusion Activities	

Table 4: CVE 2018-13379 Vulnerability Details

Fortinet FortioOS Secure Socket Layer VPN (CVE 2018-13379)	
Vulnerability Description Fortinet Secure Sockets Layer (SSL) VPN is vulnerable to unauthenticated directory traversal, which allows attackers to gain access to the sslvpn_websession file. An attacker is then able to exact clear-text usernames and passwords.	**CVSS 3.0** Critical
Vulnerability Discussion, IOCs, and Malware Campaigns Weakness in user access controls and web application directory structure allows attackers to read system files without authentication. Attackers are able to perform a HTTP GET request http://$SSLVPNTARGET?lang=/../../../..//////////dev/cmdb/sslvpn_websession. This results the server responding with unprintable/hex characters alongside cleartext credential information. *Multiple malware campaigns have taken advantage of this vulnerability. The most notable being Cring ransomware (also known as Crypt3, Ghost, Phantom, and Vjszy1lo).*	**Fix** Patch Available
Recommended Mitigations • Upgrade to the latest Fortinet SSL VPN. • Monitor for alerts to any unscheduled tasks or unknown files/executables. • Create detection/protection mechanisms that respond on directory traversal (/../../../) attempts to read the sslvpn_websessions file.	
Detection Methods • Nmap developed a script that can be used with the port scanning engine: Fortinet SSL VPN CVE-2018-13379 vuln scanner #1709.	
Vulnerable Technologies and Versions Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7, and 5.4.6 to 5.4.12 are vulnerable.	
References • FortiOS System File Leak Through SSL VPN via Specialty Crafted HTTP Resource Requests • Github: Fortinet Ssl Vpn Cve-2018-13379 Vuln Scanner #1709 • Fortinet Blog: Update Regarding CVE-2018-13379 • NIST NVD Vulnerability Detail: CVE-2018-13379 • FBI-CISA Joint Cybersecurity Advisory: Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets • FBI-CISA Joint Cybersecurity Advisory: APT Actors Exploit Vulnerabilities to Gain Initial Access for Future Attacks • NCSC Alert: Vulnerabilities Exploited in VPN Products Used Worldwide • FBI News: Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks • FBI FLASH: APT Actors Exploiting Fortinet Vulnerabilities to Gain Access for Malicious Activity	

Table 5: CVE-2020-5902 Vulnerability Details

F5 Big IP Traffic Management User Interface (CVE-2020-5902)	
Vulnerability Description The Traffic Management User Interface (TMUI), also referred to as the Configuration Utility, has an RCE vulnerability in undisclosed pages.	**CVSS 3.0** Critical

Vulnerability Discussion, IOCs, and Malware Campaigns This vulnerability allows for unauthenticated attackers, or authenticated users, with network access to the Configuration Utility (through the BIG-IP management port and/or self IPs) to execute arbitrary system commands, create or delete files, disable services, and execute arbitrary Java code. This vulnerability may result in complete system compromise. The BIG-IP system in Appliance mode is also vulnerable. This issue is not exposed on the data plane; only the control plane is affected.	**Fix** Upgrade to Secure Versions Available
Recommended Mitigations Download and install a fixed software version of the software from a vendor approved resource. If it is not possible to update quickly, restrict access via the following actions. • Address unauthenticated and authenticated attackers on self IPs by blocking all access. • Address unauthenticated attackers on management interface by restricting access.	
Detection Methods • F5 developed a free detection tool for this vulnerability: f5devcentral / cve-2020-5902-ioc-bigip-checker. • Manually check your software version to see if it is susceptible to this vulnerability.	
Vulnerable Technologies and Versions BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO, CGNAT) 15.1.0, 15.0.0-15.0.1, 14.1.0-14.1.2, 13.1.0-13.1.3, 12.1.0-12.1.5, and 11.6.1-11.6.5 are vulnerable.	
References • F5 Article: TMUI RCE Vulnerability CVE-2020-5902 • NIST NVD Vulnerability Detail: CVE-2020-5902 • CISA Alert: Threat Actor Exploitation of F5 BIG-IP CVE-2020-5902 • MITRE CVE Record: CVE-2020-5902	

Table 6: CVE-2020-15505 Vulnerability Details

MobileIron Core & Connector (CVE-2020-15505)	
Vulnerability Description MobileIron Core & Connector, Sentry, and Monitoring and Reporting Database (RDB) software are vulnerable to RCE via unspecified vectors.	**CVSS 3.0** Critical
Vulnerability Discussion, IOCs, and Malware Campaigns CVE-2020-15505 is an RCE vulnerability in MobileIron Core & Connector versions 10.3 and earlier. This vulnerability allows an external attacker, with no privileges, to execute code of their choice on the vulnerable system. As mobile device management (MDM) systems are critical to configuration management for external devices, they are usually highly permissioned and make a valuable target for threat actors. M*ultiple APTs have been observed exploiting this vulnerability to gain unauthorized access.*	**Fix** Patch Available
Recommended Mitigations • Download and install a fixed software version of the software from a vendor approved resource.	
Detection Methods • None. Manually check your software version to see if it is susceptible to this vulnerability.	
Vulnerable Technologies and Versions MobileIron Core & Connector versions 10.3.0.3 and earlier, 10.4.0.0, 10.4.0.1, 10.4.0.2, 10.4.0.3, 10.5.1.0, 10.5.2.0, and 10.6.0.0; Sentry versions 9.7.2 and earlier and 9.8.0; and Monitor and Reporting Database (RDB) version 2.0.0.1 and earlier are vulnerable.	

References
• Ivanti Blog: MobileIron Security Updates Available • CISA-FBI Joint Cybersecurity Advisory: APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations • NIST NVD Vulnerability Detail: CVE-2020-15505 • MITRE CVE Record: CVE-2020-15505 • NSA Cybersecurity Advisory: Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities

Table 7: CVE-2020-0688 Vulnerability Details

Microsoft Exchange Memory Corruption (CVE-2020-0688)	
Vulnerability Description An RCE vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory.	**CVSS 3.0** High
Vulnerability Discussion, IOCs, and Malware Campaigns CVE-2020-0688 exists in the Microsoft Exchange Server when the server fails to properly create unique keys at install time. An authenticated user with knowledge of the validation key and a mailbox may pass arbitrary objects for deserialization by the web application that runs as SYSTEM. The security update addresses the vulnerability by correcting how Microsoft Exchange creates the keys during install. A nation-state *APT actor has been observed exploiting this vulnerability to conduct widespread, distributed, and anonymized brute force access attempts against hundreds of government and private sector targets worldwide.*	**Fix** Patch Available
Recommended Mitigations • Download and install a fixed software version of the software from a vendor approved resource.	
Detection Methods • Manually check your software version to see if it is susceptible to this vulnerability. • CVE-2020-0688 is commonly exploited to install web shell malware. NSA provides guidance on detecting and preventing web shell malware at https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF and signatures at https://github.com/nsacyber/Mitigating-Web-Shells.	
Vulnerable Technologies and Versions Microsoft Exchange Server 2019 Cumulative Update 3 and 4, 2016 Cumulative Update 14 and 15, 2013 Cumulative Update 23, and 2010 Service Pack 3 Update Rollup 30 are vulnerable.	
References • Microsoft Security Update Guide: CVE-2020-0688 • NIST NVD Vulnerability Detail: CVE-2020-0688 • Microsoft Security Update: Description of the security update for Microsoft Exchange Server 2019 and 2016: February 11, 2020 • CISA-FBI Joint Cybersecurity Advisory: Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets • ACSC Alert: Active Exploitation of Vulnerability in Microsoft Internet Information Services • NSA-CISA-FBI-NCSC Cybersecurity Advisory: Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments	

Table 8: CVE-2019-3396 Vulnerability Details

Atlassian Confluence Server Widget Connector (CVE-2019-3396)	
Vulnerability Description Atlassian Confluence Server and Data Center Widget Connector is vulnerable to a server-side template injection attack.	**CVSS 3.0** Critical
Vulnerability Discussion, IOCs, and Malware Campaigns Confluence Server and Data Center versions released before June 18, 2018, are vulnerable to this issue. A remote attacker is able to exploit a server-side request forgery (SSRF) vulnerability in the WebDAV plugin to send arbitrary HTTP and WebDAV requests from a Confluence Server or Data Center instance. A successful attack is able to exploit this issue to achieve server-side template injection, path traversal, and RCE on vulnerable systems. *Multiple malware campaigns have taken advantage of this vulnerability; the most notable being GandCrab ransomware.*	**Fix** Patch Available
Recommended Mitigations • Download and install a fixed software version of the software from a vendor-approved resource.	
Detection Methods • Manually check the software version to see if it is susceptible to this vulnerability. • CVE-2019-3396 is commonly exploited to install web shell malware. NSA provides guidance on detecting and preventing web shell malware at https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF and signatures at https://github.com/nsacyber/Mitigating-Web-Shells.	
Vulnerable Technologies and Versions All versions of Confluence Server and Confluence Data Center before version 6.6.12, from version 6.7.0 before 6.12.3 (the fixed version for 6.12.x), from version 6.13.0 before 6.13.3 (the fixed version for 6.13.x), and from version 6.14.0 before 6.14.2 (the fixed version for 6.14.x) are vulnerable.	
References • NIST NVD Vulnerability Detail: CVE-2019-3396 • MITRE CVE Record: CVE-2019-3396 • Confluence Security Advisory: Confluence Data Center and Server 7.12 • Confluence Server and Data Center CONFSERVER-57974: Remote Code Execution via Widget Connector Macro - CVE-2019-3396 • TrendMicro Research Article: CVE-2019-3396: Exploiting the Confluence Vulnerability	

Table 9: CVE 2017-11882 Vulnerability Details

Microsoft Office Memory Corruption (CVE 2017-11882)	
Vulnerability Description Microsoft Office is prone to a memory corruption vulnerability allowing an attacker to run arbitrary code, in the context of the current user, by failing to properly handle objects in memory. It is also known as the "Microsoft Office Memory Corruption Vulnerability." Cyber actors continued to exploit this four-year-old vulnerability in Microsoft Office that the U.S. Government publicly assessed last year was the most frequently targeted. Cyber actors most likely continue to exploit this vulnerability because Microsoft Office use is ubiquitous worldwide, the vulnerability is ideal for phasing campaigns, and it enables RCE on vulnerable systems.	**CVSS 3.0** High

Vulnerability Discussion, IOCs, and Malware Campaigns	**Fix**
Microsoft Equation Editor, a component of Microsoft Office, contains a stack buffer overflow vulnerability that enables RCE on a vulnerable system. The component was compiled on November 9, 2000. Without any further recompilation, it was used in all currently supported versions of Microsoft Office. Microsoft Equation Editor is an out-of-process COM server that is hosted by eqnedt32.exe, meaning it runs as its own process and can accept commands from other processes. Data execution prevention (DEP) and address space layout randomization (ASLR) should protect against such attacks. However, because of the manner in which eqnedt32.exe was linked, it will not use these features, subsequently allowing code execution. Being an out-of-process COM server, protections specific to Microsoft Office such as EMET and Windows Defender Exploit Guard are not applicable to eqnedt32.exe, unless applied system-wide. This provides the attacker with an avenue to lure targets into opening specially crafted documents, resulting in the ability to execute an embedded attacker commands. *Multiple cyber espionage campaigns have taken advantage of this vulnerability. CISA has noted CVE-2017-11882 being exploited to deliver LokiBot malware.*	Patch Available
Recommended Mitigations • To remediate this issue, administrators should deploy Microsoft's patch for this vulnerability: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882. • Those who cannot deploy the patch should consider disabling the Equation Editor as discussed in Microsoft Knowledge Base Article 4055535.	
Detection Methods • Microsoft Defender Antivirus, Windows Defender, Microsoft Security Essentials, and the Microsoft Safety Scanner will all detect and patch this vulnerability.	
Vulnerable Technologies and Versions Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 are vulnerable.	
References • NIST NVD Vulnerability Detail: CVE-2017-11882 • CISA Malware Analysis Report: MAR-10211350-1.v2 • Palo Alto Networks Analysis: Analysis of CVE-2017-11882 Exploit in the Wild • CERT Coordination Center Vulnerability Note: Microsoft Office Equation Editor stack buffer overflow	

Table 10: CVE 2019-11580 Vulnerability Details

Atlassian Crowd and Crowd Data Center Remote Code Execution (CVE 2019-11580)	
Vulnerability Description Atlassian Crowd and Crowd Data Center had the pdkinstall development plugin incorrectly enabled in release builds.	**CVSS 3.0** Critical
Vulnerability Discussion, IOCs, and Malware Campaigns Attackers who can send unauthenticated or authenticated requests to a Crowd or Crowd Data Center instance can exploit this vulnerability to install arbitrary plugins, which permits RCE on systems running a vulnerable version of Crowd or Crowd Data Center.	**Fix** Patch Available
Recommended Mitigations	

• Atlassian recommends customers running a version of Crowd below version 3.3.0 to upgrade to version 3.2.8. For customers running a version above or equal to 3.3.0, Atlassian recommends upgrading to the latest version. • Released Crowd and Crowd Data Center version 3.4.4 contains a fix for this issue and is available at https://www.atlassian.com/software/crowd/download. • Released Crowd and Crowd Data Center versions 3.0.5, 3.1.6, 3.2.8, and 3.3.5 contain a fix for this issue and are available at https://www.atlassian.com/software/crowd/download-archive.
Detection Methods • Manually check your software version to see if it is susceptible to this vulnerability. • CVE-2019-11580 is commonly exploited to install web shell malware. NSA provides guidance on detecting and preventing web shell malware at https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF and signatures at https://github.com/nsacyber/Mitigating-Web-Shells.
Vulnerable Technologies and Versions All versions of Crowd from version 2.1.0 before 3.0.5 (the fixed version for 3.0.x), from version 3.1.0 before 3.1.6 (the fixed version for 3.1.x), from version 3.2.0 before 3.2.8 (the fixed version for 3.2.x), from version 3.3.0 before 3.3.5 (the fixed version for 3.3.x), and from version 3.4.0 before 3.4.4 (the fixed version for 3.4.x) are affected by this vulnerability.
References • NIST NVD Vulnerability Detail: CVE-2019-11580 • Crowd CWD-5388: Crowd – pdkinstall Development Plugin Incorrectly Enabled – CVE-2019-11580 • Crowd Security Advisory: Crowd Data Center and Server 4.3

Table 11: CVE 2018-7600 Vulnerability Details

Drupal Core Multiple Remote Code Execution (CVE 2018-7600)	
Vulnerability Description Drupal versions before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1 allow remote attackers to execute arbitrary code because of an issue affecting multiple subsystems with default or common module configurations.	**CVSS 3.0** Critical
Vulnerability Discussion, IOCs, and Malware Campaigns An RCE vulnerability exists within multiple subsystems of Drupal 7.x and 8.x. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being completely compromised. Failed exploit attempts may result in a denial-of-service condition. A remote user can send specially crafted data to trigger a flaw in the processing of renderable arrays in the Form Application Programming Interface, or API, and cause the target system to render the user-supplied data and execute arbitrary code on the target system. *Malware campaigns include the Muhstik botnet and XMRig Monero Cryptocurrency mining.*	**Fix** Patch Available
Recommended Mitigations • Upgrade to the most recent version of Drupal 7 or 8 core. If running 7.x, upgrade to Drupal 7.58. If running 8.5.x, upgrade to Drupal 8.5.1.	
Detection Methods • Dan Sharvit developed a tool to check for the CVE-2018-7600 vulnerability on several URLs: https://github.com/sl4cky/CVE-2018-7600-Masschecker/blob/master/Drupalgeddon-mass.py.	
Vulnerable Technologies and Versions • Drupal versions before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1 are affected.	

References
• Drupal Security Advisory: Drupal Core - Highly Critical - Remote Code Execution - SA-CORE-2018-002 • NIST NVD Vulnerability Detail: CVE-2018-7600 • Drupal Groups: FAQ about SA-CORE-2018-002

Table 12: CVE 2019-18935 Vulnerability Details

Telerik UI for ASP.NET AJAX Insecure Deserialization (CVE 2019-18935)	
Vulnerability Description Telerik User Interface (UI) for ASP.NET does not properly filter serialized input for malicious content. Versions prior to R1 2020 (2020.1.114) are susceptible to remote code execution attacks on affected web servers due to a deserialization vulnerability.	**CVSS 3.0** Critical
Vulnerability Discussion, IOCs, and Malware Campaigns The Telerik UI does not properly sanitize serialized data inputs from the user. This vulnerability leads to the application being vulnerable to RCE attacks that may lead to a full system compromise. A vulnerable HTTP POST parameter rauPostData makes use of a vulnerable function/object AsyncUploadHandler. The object/function uses the JavaScriptSerializer.Deserialize() method, which not not properly sanitize the serialized data during the deserialization process. This issue is attacked by: 1. Determining the vulnerable function is available/registered: http://<HOST>/Telerik.Web.UI.WebResource.axd?type=rau, 2. Determining if the version running is vulnerable by querying the UI, and 3. Creating an object (e.g., malicious mixed-mode DLL with native OS commands or Reverse Shell) and uploading the object via rauPostData parameter along with the proper encryption key. *There were two malware campaigns associated with this vulnerability:* • *Netwalker Ransomware and* • *Blue Mockbird Monero Cryptocurrency-mining.*	**Fix** Patch Available
Recommended Mitigations • Update to the most recent version of Telerik UI for ASP.NET AJAX (at least 2020.1.114 or later).	
Detection Methods • ACSC has an example PowerShell script that can be used to identify vulnerable Telerik UI DLLs on Windows web server hosts. • Vulnerable hosts should be reviewed for evidence of exploitation. Indicators of exploitation can be found in IIS HTTP request logs and within the Application Windows event log. Details of the above PowerShell script and exploitation detection recommendations are available in ACSC Advisory 2020-004. • Exploitation of this and previous Telerik UI vulnerabilities commonly resulted in the installation of web shell malware. NSA provides guidance on detecting and preventing web shell malware.	
Vulnerable Technologies and Versions Telerik UI for ASP.NET AJAX versions prior to R1 2020 (2020.1.114) are affected.	
References • Telerik UI for ASP.NET AJAX security advisory – Allows JavaScriptSerializer Deserialization • NIST NVD Vulnerability Detail: CVE-2019-18935 • ACSC Advisory 2020-004: Remote Code Execution Vulnerability Being Actively Exploited in Vulnerable Versions of Telerik UI by Sophisticated Actors • Bishop Fox – CVE-2019-18935: Remote Code Execution via Insecure Deserialization in Telerik UI • ACSC Advisory 2020-004: Remote Code Execution Vulnerability Being Actively Exploited in Vulnerable Versions of Telerik UI by Sophisticated Actors	

- FBI FLASH: Indicators Associated with Netwalker Ransomware

Table 13: CVE-2019-0604 Vulnerability Details

Microsoft SharePoint Remote Code Execution (CVE-2019-0604)	
Vulnerability Description A vulnerability in an XML deserialization component within Microsoft SharePoint allowed remote attackers to execute arbitrary code on vulnerable Microsoft SharePoint servers.	**CVSS 3.0** Critical
Vulnerability Discussion, IOCs, and Malware Campaigns This vulnerability was typically exploited to install webshell malware to vulnerable hosts. A webshell could be placed in any location served by the associated Internet Information Services (IIS) web server and did not require authentication. These web shells would commonly be installed in the Layouts folder within the Microsoft SharePoint installation directory, for example: C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\<version_number>\Template\Layouts The xmlSerializer.Deserialize() method does not adequately sanitize user input that is received from the PickerEnitity/ValidateEnity (picker.aspx) functions in the serialized XML payloads. Once the serialized XML payload is deserialized, the XML code is evaulated for relevant XML commands and stings. A user can attack .Net based XML parsers with XMLNS payloads using the <system:string> tag and embedding malicious operating system commands. *The exploit was used in malware phishing and the WickrMe/Hello Ransomware campaigns.*	**Fix** Patch Available
Recommended Mitigations • Upgrade on-premise installations of Microsoft Sharepoint to the latest available version (Microsoft SharePoint 2019) and patch level. • On-premise Microsoft SharePoint installations with a requirement to be accessed by internet-based remote staff should be moved behind an appropriate authentication mechanism such as a VPN, if possible.	
Detection Methods • The patch level of on-premise Microsoft SharePoint installations should be reviewed for the presence of relevant security updates as outlined in the Microsoft SharePoint security advisory. • Vulnerable SharePoint servers should be reviewed for evidence of attempted exploitation. ACSC Advisory 2019-125 contains advice on reviewing IIS HTTP request logs for evidence of potential exploitation. • NSA provides guidance on detecting and preventing web shell malware.	
Vulnerable Technologies and Versions At the time of the vulnerability release, the following Microsoft SharePoint versions were affected: Microsoft Sharepoint 2019, Microsoft SharePoint 2016, Microsoft SharePoint 2013 SP1, and Microsoft SharePoint 2010 SP2.	
References • Microsoft – SharePoint Remote Code Execution Vulnerability Security Advisory • NIST NVD Vulnerability Detail: CVE-2019-0604 • ACSC Advisory 2019-125: Targeting of Microsoft SharePoint CVE-2019-0604	

- NSCS Alert: Microsoft SharePoint Remote Code Vulnerability

Table 14: CVE-2020-0787 Vulnerability Details

Windows Background Intelligent Transfer Service Elevation of Privilege (CVE-2020-0787)	
Vulnerability Description The Windows Background Intelligent Transfer Service (BITS) is vulnerable to a privilege elevation vulnerability if it improperly handles symbolic links. An actor can exploit this vulnerability to execute arbitrary code with system-level privileges.	**CVSS 3.0** High
Vulnerability Discussion, IOCs, and Malware Campaigns To exploit this vulnerability, an actor would first need to have the ability to execute arbitrary code on a vulnerable Windows host. Actors exploiting this vulnerability commonly used the proof of concept code released by the security researcher who discovered the vulnerability. If an actor left the proof of concept exploit's working directories unchanged, then the presence of the following folders could be used as an indicator of exploitation: C:\Users\<username>\AppData\Local\Temp\workspace C:\Users\<username>\AppData\Local\Temp\workspace\mountpoint C:\Users\<username>\AppData\Local\Temp\workspace\bait *The exploit was used in Maze and Egregor ransomware campaigns.*	**Fix** Patch Available
Recommended Mitigations • Apply the security updates as recommended in the Microsoft Netlogon security advisory.	
Detection Methods • The patch level of all Microsoft Windows installations should be reviewed for the presence of relevant security updates as outlined in the Microsoft BITS security advisory.	
Vulnerable Technologies and Versions Windows 7 for 32-bit and x64-based Systems Service Pack 1, 8.1 for 32-bit and x64-based systems, RT 8.1, 10 for 32-bit and x64-based Systems, 10 1607 for 32-bit and x64-based Systems, 10 1709 for 32-bit and x64-based and ARM64-based Systems, 10 1803 for 32-bit and ARM64-based and x64-based Systems, 10 1809 for 32-bit and ARM64-based and x64-based Systems, 10 1903 for 32-bit and ARM64-based and x64-based Systems, 10 1909 for 32-bit, and ARM64-based and x64-based Systems are vulnerable. Windows Server 2008 R2 for x64-based Systems Service Pack 1, 2008 R2 for x64-based Systems Service Pack 1 (Server Core Installation), 2008 for 32-bit Systems Service Pack 2, 2008 for 32-bit Systems Service Pack 2 (Server Core Installation), 2012, 2012 (Server Core Installation), 2012 R2, 2012 R2 (Server Core Installation), 2016, 2016 (Server Core Installation), 2019, 2019 (Server Core Installation), 1803 (Server Core Installation), 1903 (Server Core Installation), and 1909 (Server Core Installation) are also vulnerable.	
References • Microsoft – Windows Background Intelligent Transfer Service Elevation of Privilege Security Advisory • NIST NVD Vulnerability Detail: CVE-2020-0787 • Security Researcher – Proof of Concept Exploit Code	

Table 15: CVE-2020-1472 Vulnerability Details

Netlogon Elevation of Privilege (CVE-2020-1472)	
Vulnerability Description The Microsoft Windows Netlogon Remote Protocol (MS-NRPC) reuses a known, static, zero-value initialization vector (VI) in AES-CFB8 mode, which could allow an unauthenticated attacker to impersonate a domain-joined computer including a domain controller, and potentially obtain domain administrator privileges.	**CVSS 3.0** Critical
Vulnerability Discussion, IOCs, and Malware Campaigns To exploit this vulnerability, an actor would first need to have an existing presence on an internal network with network connectivity to a vulnerable Domain Controller, assuming that Domain Controllers are not exposed to the internet. The immediate effect of successful exploitation results in the ability to authentication to the vulnerable Domain Controller with Domain Administrator level credentials. In compromises exploiting this vulnerability, exploitation was typically followed immediately by dumping all hashes for Domain accounts. Threat actors were seen combining the MobileIron CVE-2020-15505 vulnerability for initial access, then using the Netlogon vulnerability to facilitate lateral movement and further compromise of target networks. A nation-state *APT group has been observed exploiting this vulnerability.[18]*	**Fix** Patch Available
Recommended Mitigations • Apply the security updates as recommended in the Microsoft Netlogon security advisory.	
Detection Methods • The patch level of Domain Controllers should be reviewed for the presence of relevant security updates as outlined in the Microsoft Netlogon security advisory. • Reviewing and monitoring Windows Event Logs can identify potential exploitation attempts. However, further investigation would still be required to eliminate legitimate activity. Further information on these event logs is available in the ACSC 2020-016 Advisory.	
Vulnerable Technologies and Versions At the time of the vulnerability release, the following Microsoft Windows Server versions were vulnerable: all versions of Windows Server 2019; all versions of Windows Server 2016; Windows Server 2012 R2; Windows Server 2012; Windows Server 2008 R2 SP1; and Windows Server versions 1909/1903/1809.	
References • Microsoft – Netlogon Elevation of Privilege Vulnerability • NIST NVD Vulnerability Detail: CVE-2020-1472 • ACSC 2020-016 Netlogon Advisory • CISA-FBI Joint Cybersecurity Advisory: APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations • CISA-FBI Joint Cybersecurity Advisory: Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets • ACSC Advisory 2020-016: "Zerologon" – Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) • NCSC Alert: UK Organisations Should Patch Netlogon Vulnerability (Zerologon)	

For additional general best practices for mitigating cyber threats, see the joint advisory from Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity and ACSC's Essential Eight mitigation strategies.

ADDITIONAL RESOURCES

Free Cybersecurity Services

CISA offers several free cyber hygiene vulnerability scanning and web application services to help U.S. federal agencies, state and local governments, critical infrastructure, and private organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. For more information about CISA's free services, or to sign up, email vulnerability_info@cisa.dhs.gov.

Cyber Essentials

CISA's Cyber Essentials is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.

Cyber.gov.au

ACSC's website provides advice and information about how to protect individuals and families, small- and medium-sized businesses, large organizations and infrastructure, and government organizations from cyber threats.

ACSC Partnership Program

The ACSC Partnership Program enables Australian organizations and individuals to engage with ACSC and fellow partners, drawing on collective understanding, experience, skills, and capability to lift cyber resilience across the Australian economy.

Australian organizations, including government and those in the private sector as well individuals, are welcome to sign up at Become an ACSC partner to join.

NCSC 10 Steps

The NCSC offers 10 Steps to Cyber Security, providing detailed guidance on how medium and large organizations can manage their security.

On vulnerabilities specifically, the NCSC has guidance to organizations on establishing an effective vulnerability management process, focusing on the management of widely available software and hardware.

REFERENCES

[1] NSA-CISA-FBI Cybersecurity Advisory: Russian SVR Targets U.S. and Allied Networks

[2] CISA-FBI-NSA-NCSC Advisory: Further TTPs Associated with SVR Cyber Actors

[3] NSA Cybersecurity Advisory: Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities

[4] ACSC Advisory 2020-001-4: Remediation for Critical Vulnerability in Citrix Application Delivery Controller and Citrix Gateway

[5] NCSC Alert: Actors Exploiting Citrix Products Vulnerability

[6] Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets

[7] CISA-FBI Joint Cybersecurity Advisory: Top 10 Routinely Exploited Vulnerabilities

[8] ACSC Alert: APT Exploitation of Fortinet Vulnerabilities

[9] NCSC Alert: Alert: Critical Risk to Unpatched Fortinet VPN Devices

[10] NSA Cybersecurity Advisory: Mitigating Recent VPN Vulnerabilities

[11] NCSC Alert: Vulnerabilities Exploited in VPN Products Used Worldwide

[12] NCSC-Canada's Communications Security Establishment-NSA-CISA Advisory: APT29 Targets COVID-19 Vaccine Development (CSE)

[13] ACSC Advisory: Summary of Tactics, Techniques and Procedures Used to Target Australian Networks

[14] CISA Alert: Continued Exploitation of Pulse Secure VPN Vulnerability

[15] CISA Alert: Continued Threat Actor Exploitation Post Pulse Secure VPN Patching

[16] CISA Emergency Directive (ED 20-03): Windows DNS Server Vulnerability

[17] NCSC Alert: Alert: Multiple Actors are Attempting to Exploit MobileIron Vulnerability CVE 2020-15505

[18] NJCCIC Alert: APT10 Adds ZeroLogon Exploitation to TTPs