Potential for China Cyber Response to Heightened U.S.–China Tensions

us-cert.cisa.gov/ncas/alerts/aa20-275a

Summary

This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor techniques.

***Note**: on October 20, 2020, the National Security Agency (NSA) released a cybersecurity advisory providing information on publicly known vulnerabilities exploited by Chinese state-sponsored cyber actors to target computer networks holding sensitive intellectual property, economic, political, and military information. This Alert has been updated to include information on vulnerabilities exploited by Chinese state-sponsored actors (see Table 4).*

In light of heightened tensions between the United States and China, the Cybersecurity and Infrastructure Security Agency (CISA) is providing specific Chinese government and affiliated cyber threat actor tactics, techniques, and procedures (TTPs) and recommended mitigations to the cybersecurity community to assist in the protection of our Nation's critical infrastructure. In addition to the recommendations listed in the Mitigations section of this Alert, CISA recommends organizations take the following actions.

1. **Adopt a state of heightened awareness.** Minimize gaps in personnel availability, consistently consume relevant threat intelligence, and update emergency call trees.
2. **Increase organizational vigilance.** Ensure security personnel monitor key internal security capabilities and can identify anomalous behavior. Flag any known Chinese indicators of compromise (IOCs) and TTPs for immediate response.
3. **Confirm reporting processes.** Ensure personnel know how and when to report an incident. The well-being of an organization's workforce and cyber infrastructure depends on awareness of threat activity. Consider reporting incidents to CISA to help serve as part of CISA's early warning system (see the Contact Information section below).
4. **Exercise organizational incident response plans.** Ensure personnel are familiar with the key steps they need to take during an incident. Do they have the accesses they need? Do they know the processes? Are various data sources logging as expected? Ensure personnel are positioned to act in a calm and unified manner.

Technical Details

China Cyber Threat Profile

China has a history of using national military and economic resources to leverage offensive cyber tactics in pursuing its national interests. The “Made in China 2025” 10-year plan outlines China’s top-level policy priorities.[1],[2] China may seek to target the following industries deemed critical to U.S. national and economic interests: new energy vehicles, next generation information technology (IT), biotechnology, new materials, aerospace, maritime engineering and high-tech ships, railway, robotics, power equipment, and agricultural machinery.[3] China has exercised its increasingly sophisticated capabilities to illegitimately obtain U.S. intellectual property (IP), suppress both social and political perspectives deemed dangerous to China, and harm regional and international opponents.

The U.S. Intelligence Community and various private sector threat intelligence organizations have identified the Chinese People’s Liberation Army (PLA) and Ministry of State Security (MSS) as driving forces behind Chinese state-sponsored cyberattacks–either through contractors in the Chinese private sector or by the PLA and MSS entities themselves. China continues to engage in espionage-related activities that include theft of sensitive information such as innovation capital, IP, and personally identifiable information (PII). China has demonstrated a willingness to push the boundaries of their activities to secure information critical to advancing their economic prowess and competitive advantage.

Chinese Cyber Activity

According to open-source reporting, offensive cyber operations attributed to the Chinese government targeted, and continue to target, a variety of industries and organizations in the United States, including healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, IT, international trade, education, videogaming, faith-based organizations, and law firms.

Additionally, numerous Department of Justice (DOJ) indictments over several years provide evidence to suggest Chinese threat actors continuously seek to illegally obtain and exfiltrate U.S. IP. Their targets also include western companies with operations inside China.

Public reporting that associates Chinese actors with a range of high-profile attacks and offensive cyber activity includes:

- **February 2013 – Cyber Threat Intelligence Researchers Link Advanced Persistent Threat (APT) 1 to China:** a comprehensive report publicly exposed APT1 as part of China’s military cyber operations and a multi-year effort that exfiltrated IP from roughly 141 companies spanning 20 major industries.[4] APT1 established access to the victims’ networks and methodically exfiltrated IP across a large range of industries identified in China’s 12th 5-Year Plan. A year later, the DOJ indicted Chinese cyber threat actors assigned to PLA Unit 61398 for the first time (also highlighted in the report).[5]

- **April 2017 – Chinese APTs Targeting IP in 12 Countries:** CISA announced Chinese state-backed APTs carried out a multi-year campaign of cyber-enabled IP theft that targeted global technology service providers and their customers. The threat actors leveraged stolen administrative credentials (local and domain) and placed sophisticated malware on critical systems in an effort to steal the IP and sensitive data of companies located in at least 12 countries.[6]
- **December 2018 – Chinese Cyber Threat Actors Indicted for Compromising Managed Service Providers (MSPs):** DOJ indicted two Chinese cyber threat actors believed to be associated with APT10, who targeted MSPs and their large customer base through phishing and spearphishing campaigns aimed at exfiltrating sensitive business data and, possibly, PII.[7] CISA also briefed stakeholders on Chinese APT groups who targeted MSPs and their customers to steal data and further operationalize commercial and economic espionage.[8]
- **February 2020 – China's Military Indicted for 2017 Equifax Hack:** DOJ indicted members of China's PLA for stealing large amounts of PII and IP. The Chinese cyber threat actors exploited a vulnerability in the company's dispute resolution website to enter the network, conduct reconnaissance, upload malware, and steal credentials to extract the targeted data. The breach impacted roughly half of all American citizens and stole Equifax's trade secrets.[9]
- **May 2020 – China Targets COVID-19 Research Organizations:** the Federal Bureau of Investigation (FBI) and CISA reported the targeting and compromise of U.S. organizations conducting COVID-19-related research by cyber actors affiliated with China.[10] Large-scale password spraying campaigns were a commonly observed tactic in illicitly obtaining IP related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research.[11],[12]

Common TTPs of Publicly Known Chinese Threat Actors

The section below provides common, publicly known, TTPs employed by Chinese threat actors, which map to the MITRE ATT&CK framework. Where possible, the tables include actions for detection and mitigation. This section is not exhaustive and does not detail all TTPs or detection and mitigation actions.

PRE-ATT&CK TTPs

Chinese threat actors commonly use the techniques listed in table 1 to achieve reconnaissance (*Technical Information Gathering* [TA0015]), staging (*Stage Capabilities* [TA0026]), and testing (*Test Capabilities* [TA0025]) before executing an attack. PRE-ATT&CK techniques can be difficult to detect and mitigate, however, defenders should be aware of the use of these techniques.

Table 1: Chinese threat actor PRE-ATT&CK techniques

Technique	Description

Technique	Description
Acquire and/or Use 3rd Party Software Services [T1330]	Staging and launching attacks from software as a service solutions that cannot be easily tied back to the APT
Compromise 3rd Party Infrastructure to Support Delivery [T1334]	Compromising infrastructure owned by other parties to facilitate attacks (instead of directly purchasing infrastructure)
Domain Registration Hijacking [T1326]	Changing the registration of a domain name without the permission of its original registrant and then using the legitimate domain as a launch point for malicious purposes
Acquire Open-Source Intelligence (OSINT) Data Sets and Information [T1247]	Gathering data and information from publicly available sources, including public-facing websites of the target organization
Conduct Active Scanning [T1254]	Gathering information on target systems by scanning the systems for vulnerabilities. Adversaries are likely using tools such as Shodan to identify vulnerable devices connected to the internet
Analyze Architecture and Configuration Posture [T1288]	Analyzing technical scan results to identify architectural flaws, misconfigurations, or improper security controls in victim networks
Upload, Install, and Configure Software/Tools [T1362]	Placing malware on systems illegitimately for use during later stages of an attack to facilitate exploitability and gain remote access

Enterprise ATT&CK TTPs

Chinese threat actors often employ publicly known TTPs against enterprise networks. To orchestrate attacks, they use commonly implemented security testing tools and frameworks, such as:

- Cobalt Strike and Beacon
- Mimikatz
- PoisonIvy
- PowerShell Empire
- China Chopper Web Shell

Table 2 lists common, publicly known, TTPs used by Chinese threat actors against enterprise networks and provides options for detection and mitigation based on the MITRE ATT&CK framework.

Table 2: Common Chinese threat actor techniques, detection, and mitigation

Technique / Sub-Technique	**Detection**	**Mitigation**
Obfuscated Files or Information [T1027]	- Detect obfuscation by analyzing signatures of modified files. - Flag common syntax used in obfuscation.	Use antivirus/antimalware software to analyze commands after processing.
Phishing: Spearphishing Attachment [T1566.001] and *Spearphishing Link* [T1566.002]	- Use network intrusion detection systems (NIDS) and email gateways to detect suspicious attachments in email entering the network. - Use detonation chambers to inspect email attachments in isolated environments.	- Quarantine suspicious files with antivirus solutions. - Use network intrusion prevention systems to scan and remove malicious email attachments. - Train users to identify phishing emails and notify IT.
System Network Configuration Discovery [T1016]	Monitor for processes and command-line arguments that could be used by an adversary to gather system and network information.	This technique is difficult to mitigate with preventative controls; organizations should focus on detecting and responding to malicious activity to limit impact.
Command and Scripting Interpreter: Windows Command Shell [T1059.003]	Identify normal scripting behavior on the system then monitor processes and command-line arguments for suspicious script execution behavior.	- Only permit execution of signed scripts. - Disable any unused shells or interpreters.
User Execution: Malicious File [T1204.002]	- Monitor execution of command-line arguments for applications (including compression applications) that may be used by an adversary to execute a user interaction. - Set antivirus software to detect malicious documents and files downloaded and installed on endpoints.	- Use execution prevention to prevent the running of executables disguised as other files. - Train users to identify phishing attacks and other malicious events that may require user interaction.

Technique / Sub-Technique	Detection	Mitigation
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547.001]	- Monitor the start folder for additions and changes. - Monitor registry for changes to run keys that do not correlate to known patches or software updates.	This technique is difficult to mitigate with preventative controls; organizations should focus on detecting and responding to malicious activity to limit impact.
Command and Scripting Interpreter: PowerShell [T1059.001]	- Enable PowerShell logging. - Monitor for changes in PowerShell execution policy as a method of identifying malicious use of PowerShell. - Monitor for PowerShell execution generally in environments where PowerShell is not typically used.	- Set PowerShell execution policy to execute only signed scripts. - Disable PowerShell if not needed by the system. - Disable WinRM service to help prevent use of PowerShell for remote execution. - Restrict PowerShell execution policy to administrators.
Hijack Execution Flow: DLL Side-Loading [T1574.002]	Track Dynamic Link Library (DLL) metadata, and compare DLLs that are loaded at process execution time against previous executions to detect usual differences unrelated to patching.	- Use the program `sxstrace.exe` to check manifest files for side-loading vulnerabilities in software. - Update software regularly including patches for DLL side-loading vulnerabilities.
Ingress Tool Transfer [T1105]	- Monitor for unexpected file creation or files transfer into the network from external systems, which may be indicative of attackers staging tools in the compromised environment. - Analyze network traffic for unusual data flows (i.e., a client sending much more data than it receives from a server).	Use network intrusion detection and prevention systems to identify traffic for specific adversary malware or unusual data transfer over protocols such as File Transfer Protocol.

Technique / Sub-Technique	Detection	Mitigation
Remote System Discovery [T1018]	• Monitor processes and command-line arguments for actions that could be taken to gather system and network information. • In cloud environments, usage of commands and application program interfaces (APIs) to request information about remote systems combined with additional unexpected commands may be a sign of malicious use.	This technique is difficult to mitigate with preventative controls; organizations should focus on detecting and responding to malicious activity to limit impact.
Software Deployment Tools [T1072]	Identify the typical use pattern of third-party deployment software, then monitor for irregular deployment activity.	• Isolate critical network systems access using group policies, multi-factor authentication (MFA), and firewalls. • Patch deployment systems regularly. • Use unique and limited credentials for access to deployment systems.
Brute Force: Password Spraying [T1110.003]	Monitor logs for failed authentication attempts to valid accounts.	• Use MFA. • Set account lockout policies after a certain number of failed login attempts.
Network Service Scanning [T1046]	Use NIDS to identify scanning activity.	• Close unnecessary ports and services. • Segment network to protect critical servers and devices.
Email Collection [T1114]	Monitor processes and command-line arguments for actions that could be taken to gather local email files.	• Encrypt sensitive emails. • Audit auto-forwarding email rules regularly. • Use MFA for public-facing webmail servers.

Technique / Sub-Technique	Detection	Mitigation
Proxy: External Proxy [T1090.002]	Analyze network data for uncommon data flows, such as a client sending significantly more data than it receives from an external server.	Use NIDS and prevention systems to identify traffic for specific adversary malware using network signatures.
Drive-by Compromise [T1189]	• Use Firewalls and proxies to inspect URLs for potentially known-bad domains or parameters. • Monitor network intrusion detection systems (IDS) to detect malicious scripts, and monitor endpoints for abnormal behavior.	• Isolate and sandbox impacted systems and applications to restrict the spread of malware. • Leverage security applications to identify malicious behavior during exploitation. • Restrict web-based content through ad-blockers and script blocking extensions.
Server Software Component: Web Shell [T1505.003]	Analyze authentication logs, files, netflow/enclave netflow, and leverage process monitoring to discover anomalous activity.	• Patch vulnerabilities in internet facing applications. • Leverage file integrity monitoring to identify file changes. • Configure server to block access to the web accessible directory through principle of least privilege.
Application Layer Protocol: File Transfer Protocols [T1071.002] and *DNS* [T1071.004]	• Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). • Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.	Leverage NIDS and NIPS using network signatures to identify traffic for specific adversary malware.

Additional APT Activity

The TTPs listed above have been repeatedly used across the spectrum of Chinese threat actors. The mitigations referenced in this alert can help reduce vulnerability to these TTPs; however, defenders should also maintain heightened awareness of threats actors that are more innovative in their approach, making it difficult to detect and respond to compromise. Publicly reported examples[13] include:

- **APT3** (known as UPS Team) is known for deploying zero-day attacks that target Internet Explorer, Firefox, and Adobe Flash Player. The group's custom implants and changing Command and Control (C2) infrastructure make them difficult to track. APT3 exploits use Rivest Cypher 4 (RC4) encryption to communicate and bypass address space layout randomization (ASLR)/Data Execution Prevention (DEP) by using Return Oriented Programming (ROP) chains.[14]
- **APT10** (known as MenuPass Group) has established accessed to victim networks through compromised service providers, making it difficult for network defenders to identify the malicious traffic.
- **APT19** (known as Codoso and Deep Panda) is known for developing custom Rich Text Format (RTF) and macro-enabled Microsoft Office documents for both implants and payloads. The group has backdoored software, such as software serial generators, and has an elite use of PowerShell for C2 over Hyper Text Transfer Protocol (HTTP)/Hyper Text Transfer Protocol Secure (HTTPS).[15]
- **APT40** (known as Leviathan) has targeted external infrastructure with success, including internet-facing routers and virtual private networks.
- **APT41** (known as Double Dragon) has exploited vulnerabilities in Citrix NetScaler/ADC, Cisco routers, and Zoho ManageEngine Desktop Central to compromise victims.[16]

Mitigations

Recommended Actions

The following list provides actionable technical recommendations for IT security professionals to reduce their organization's overall vulnerability. These recommendations are not exhaustive; rather they focus on the actions that will greatly reduce stakeholders' attack surface.

1. **Patch systems and equipment promptly and diligently.** Establishing and consistently maintaining a thorough patching cycle continues to be the best defense against adversary TTPs. Focus on patching critical and high vulnerabilities that allow for remote code execution or denial-of-service on externally-facing (i.e., internet) equipment. Certain vulnerabilities—including CVE-2012-0158 in Microsoft products [17], CVE-2019-19781 in Citrix devices [18], and CVE-2020-5902 in BIG-IP Traffic Management User Interface [19]—have presented APTs with prime targets to gain initial access. Chinese APTs often use existing exploit code to target routinely exploited vulnerabilities [20], which present an opportunistic attack that requires limited resources. See table 3 for patch information on CVEs that have been routinely exploited by Chinese APTs. See table 4 for patch information on vulnerabilities that the National Security Agency (NSA) has stated are actively used by Chinese state-sponsored cyber actors.

Table 3: Patch information for vulnerabilities routinely exploited by Chinese APT actors

Vulnerability	Vulnerable Products	Patch Information
CVE-2012-0158	Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2003 Web Components SP3; SQL Server 2000 SP4, 2005 SP4, and 2008 SP2, SP3, and R2; BizTalk Server 2002 SP1; Commerce Server 2002 SP4, 2007 SP2, and 2009 Gold and R2; Visual FoxPro 8.0 SP1 and 9.0 SP2; and Visual Basic 6.0	Microsoft Security Bulletin MS12-027: Vulnerability in Windows Common Controls Could Allow Remote Code Execution
CVE-2020-5902	Big-IP devices (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO, CGNAT)	F5 Security Advisory: K52145254: TMUI RCE vulnerability CVE-2020-5902

Vulnerability	Vulnerable Products	Patch Information
CVE-2019-19781	- Citrix Application Delivery Controller - Citrix Gateway - Citrix SDWAN WANOP	- Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway versions 11.1 and 12.0 - Citrix blog post: security updates for Citrix SD-WAN WANOP release 10.2.6 and 11.0.3 - Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway versions 12.1 and 13.0 - Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway version 10.5
CVE-2019-11510	- Pulse Connect Secure 9.0R1 - 9.0R3.3, 8.3R1 - 8.3R7, 8.2R1 - 8.2R12, 8.1R1 - 8.1R15 - Pulse Policy Secure 9.0R1 - 9.0R3.1, 5.4R1 - 5.4R7, 5.3R1 - 5.3R12, 5.2R1 - 5.2R12, 5.1R1 - 5.1R15	Pulse Secure Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX
CVE-2019-16920	D-Link products DIR-655C, DIR-866L, DIR-652, DHP-1565, DIR-855L, DAP-1533, DIR-862L, DIR-615, DIR-835, and DIR-825	D-Link Security Advisory: DAP-1533 Rv Ax, DGL-5500 Rv Ax, DHP-1565 Rv Ax, DIR-130 Rv Ax, DIR-330 Rv Ax, DIR-615 Rv Ix, (non-US) DIR-652 Rv Bx, DIR-655 Rv Cx, DIR-825 Rv Cx, DIR-835 Rv Ax, DIR-855L Rv Ax, (non-US) DIR-862 Rv Ax, DIR-866L Rv Ax :: CVE-2019-16920 :: Unauthenticated Remote Code Execution (RCE) Vulnerability
CVE-2019-16278	Nostromo 1.9.6 and below	- Nostromo 1.9.6 Directory Traversal/ Remote Command Execution - Nostromo 1.9.6 Remote Code Execution

Vulnerability	Vulnerable Products	Patch Information
CVE-2019-1652	Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers	Cisco Security Advisory: Cisco Small Business RV320 and RV325 Routers Command Injection Vulnerability
CVE-2019-1653	Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers	Cisco Security Advisory: Cisco Small Business RV320 and RV325 Routers Information Disclosure Vulnerability
CVE-2020-10189	Zoho ManageEngine Desktop Central before 10.0.474	ManageEngine Desktop Central remote code execution vulnerability (CVE-2020-10189)

Table 4: Patch information for NSA listed vulnerabilities used by Chinese state-sponsored cyber actors [21]

Vulnerability	Vulnerable Products	Patch Information
CVE-2020-8193	• Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 • Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7	Citrix Security Bulletin CTX276688
CVE-2020-8195	• Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 • Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7	Citrix Security Bulletin CTX276688
CVE-2020-8196	• Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 • Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7	Citrix Security Bulletin CTX276688

Vulnerability	Vulnerable Products	Patch Information
CVE-2019-0708	• Windows 7 for 32-bit Systems Service Pack 1 • Windows 7 for x64-based Systems Service Pack 1 • Windows Server 2008 for 32-bit Systems Service Pack 2 • Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) • Windows Server 2008 for Itanium-Based Systems Service Pack 2 • Windows Server 2008 for x64-based Systems Service Pack 2 • Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) • Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 • Windows Server 2008 R2 for x64-based Systems Service Pack 1 • Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Microsoft Security Advisory for CVE-2019-0708
CVE-2020-15505	• 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; • Monitor and Reporting Database (RDB) version 2.0.0.1 and earlier	MobileIron Blog: MobileIron Security Updates Available

Vulnerability	Vulnerable Products	Patch Information
CVE-2020-1350	- Windows Server 2008 for 32-bit Systems Service Pack 2 - Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) - Windows Server 2008 for x64-based Systems Service Pack 2 - Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) - Windows Server 2008 R2 for x64-based Systems Service Pack 1 - Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) - Windows Server 2012 - Windows Server 2012 (Server Core installation) - Windows Server 2012 R2 - Windows Server 2012 R2 (Server Core installation) - Windows Server 2016 - Windows Server 2016 (Server Core installation) - Windows Server 2019 - Windows Server 2019 (Server Core installation) - Windows Server, version 1903 (Server Core installation) - Windows Server, version 1909 (Server Core installation) - Windows Server, version 2004 (Server Core installation)	Microsoft Security Advisory for CVE-2020-1350

Vulnerability	Vulnerable Products	Patch Information
CVE-2020-1472	- Windows Server 2008 R2 for x64-based Systems Service Pack 1 - Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) - Windows Server 2012 - Windows Server 2012 (Server Core installation) - Windows Server 2012 R2 - Windows Server 2016 - Windows Server 2019 - Windows Server 2019 (Server Core installation) - Windows Server, version 1903 (Server Core installation) - Windows Server, version 1909 (Server Core installation) - Windows Server, version 2004 (Server Core installation)	Microsoft Security Advisory for CVE-2020-1472
CVE-2020-1040	- Windows Server 2008 R2 for x64-based Systems Service Pack 1 - Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) - Windows Server 2012 - Windows Server 2012 (Server Core installation) - Windows Server 2012 R2 - Windows Server 2012 R2 (Server Core installation) - Windows Server 2016 - Windows Server 2016 (Server Core installation)	Microsoft Security Advisory for CVE-2020-1040
CVE-2018-6789	Exim before 4.90.1	- Exim page for CVE-2020-6789 - Exim patch information for CVE-2020-6789

Vulnerability	Vulnerable Products	Patch Information
CVE-2020-0688	• Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 30 • Microsoft Exchange Server 2013 Cumulative Update 23 • Microsoft Exchange Server 2016 Cumulative Update 14 • Microsoft Exchange Server 2016 Cumulative Update 15 • Microsoft Exchange Server 2019 Cumulative Update 3 • Microsoft Exchange Server 2019 Cumulative Update 4	Microsoft Security Advisory for CVE-2020-0688
CVE-2018-4939	• ColdFusion Update 5 and earlier versions • ColdFusion 11 Update 13 and earlier versions	Adobe Security Bulletin APSB18-14
CVE-2015-4852	Oracle WebLogic Server 10.3.6.0, 12.1.2.0, 12.1.3.0, and 12.2.1.0	Oracle Critical Patch Update Advisory - October 2016
CVE-2020-2555	Oracle Coherence product of Oracle Fusion Middleware Middleware; versions 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0.	Oracle Critical Patch Update Advisory - January 2020
CVE-2019-3396	Atlassian Confluence Server before version 6.6.12, from version 6.7.0 before 6.12.3, from version 6.13.0 before 6.13.3), and from version 6.14.0 before 6.14.2	Jira Atlassian Confluence Sever and Data Center: Remote code execution via Widget Connector macro - CVE-2019-3396
CVE-2019-11580	Atlassian Crowd and Crowd Data Center from version 2.1.0 before 3.0.5, from version 3.1.0 before 3.1.6, from version 3.2.0 before 3.2.8, from version 3.3.0 before 3.3.5, and from version 3.4.0 before 3.4.4	Jira Atlassian Crowd: Crowd - pdkinstall development plugin incorrectly enabled - CVE-2019-11580

Vulnerability	Vulnerable Products	Patch Information
CVE-2020-10189	Zoho ManageEngine Desktop Central before 10.0.474	ManageEngine Desktop Central remote code execution vulnerability (CVE-2020-10189)
CVE-2019-18935	Progress Telerik UI for ASP.NET AJAX through 2019.3.1023	Telerik: ASP.NET AJAX: Allows JavaScriptSerializer Deserialization

Vulnerability	Vulnerable Products	Patch Information
CVE-2020-0601	• Windows 10 for 32-bit Systems • Windows 10 for x64-based Systems • Windows 10 Version 1607 for 32-bit Systems • Windows 10 Version 1607 for x64-based Systems • Windows 10 Version 1709 for 32-bit Systems • Windows 10 Version 1709 for ARM64-based Systems • Windows 10 Version 1709 for x64-based Systems • Windows 10 Version 1803 for 32-bit Systems • Windows 10 Version 1803 for ARM64-based Systems • Windows 10 Version 1803 for x64-based Systems • Windows 10 Version 1809 for 32-bit Systems • Windows 10 Version 1809 for ARM64-based Systems • Windows 10 Version 1809 for x64-based Systems • Windows 10 Version 1903 for 32-bit Systems • Windows 10 Version 1903 for ARM64-based Systems • Windows 10 Version 1903 for x64-based Systems • Windows 10 Version 1909 for 32-bit Systems • Windows 10 Version 1909 for ARM64-based Systems • Windows 10 Version 1909 for x64-based Systems • Windows Server 2016 • Windows Server 2016 (Server Core installation) • Windows Server 2019 • Windows Server 2019 (Server Core installation) • Windows Server, version 1803 (Server Core Installation) • Windows Server, version 1903 (Server Core installation) • Windows Server, version 1909 (Server Core installation)	Microsoft Security Advisory for CVE-2020-0601

Vulnerability	Vulnerable Products	Patch Information
CVE-2019-0803	• Windows 10 for 32-bit Systems • Windows 10 for x64-based Systems • Windows 10 Version 1607 for 32-bit Systems • Windows 10 Version 1607 for x64-based Systems • Windows 10 Version 1703 for 32-bit Systems • Windows 10 Version 1703 for x64-based Systems • Windows 10 Version 1709 for 32-bit Systems • Windows 10 Version 1709 for ARM64-based Systems • Windows 10 Version 1709 for x64-based Systems • Windows 10 Version 1803 for 32-bit Systems • Windows 10 Version 1803 for ARM64-based Systems • Windows 10 Version 1803 for x64-based Systems • Windows 10 Version 1809 for 32-bit Systems • Windows 10 Version 1809 for ARM64-based Systems • Windows 10 Version 1809 for x64-based Systems • Windows 7 for 32-bit Systems Service Pack 1 • Windows 7 for x64-based Systems Service Pack 1 • Windows 8.1 for 32-bit systems • Windows 8.1 for x64-based systems • Windows RT 8.1 • Windows Server 2008 for 32-bit Systems Service Pack 2 • Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) • Windows Server 2008 for Itanium-Based Systems Service Pack 2 • Windows Server 2008 for x64-based Systems Service Pack • Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) • Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	Microsoft Security Advisory for CVE-2019-0803

Vulnerability	Vulnerable Products	Patch Information
	• Windows Server 2008 R2 for x64-based Systems Service Pack 1 • Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) • Windows Server 2012 • Windows Server 2012 (Server Core installation) • Windows Server 2012 R2 • Windows Server 2012 R2 (Server Core installation) • Windows Server 2016 • Windows Server 2016 (Server Core installation) • Windows Server 2019 • Windows Server 2019 (Server Core installation) • Windows Server, version 1803 (Server Core Installation)	
CVE-2017-6327	Symantec Messaging Gateway before 10.6.3-267	Broadcom Security Updates Detial for CVE-2017-6327 and CVE-2017-6328
CVE-2020-3118	• ASR 9000 Series Aggregation Services Routers • Carrier Routing System (CRS) • IOS XRv 9000 Router • Network Convergence System (NCS) 540 Series Routers • NCS 560 Series Routers • NCS 1000 Series Routers • NCS 5000 Series Routers • NCS 5500 Series Routers • NCS 6000 Series Routers	Cisco Security Advisory cisco-sa-20200205-iosxr-cdp-rce
CVE-2020-8515	DrayTek Vigor2960 1.3.1_Beta, Vigor3900 1.4.4_Beta, and Vigor300B 1.3.3_Beta, 1.4.2.1_Beta, and 1.4.4_Beta devices	Draytek Security Advisory: Vigor3900 / Vigor2960 / Vigor300B Router Web Management Page Vulnerability (CVE-2020-8515)

1. **Implement rigorous configuration management programs.** Audit configuration management programs to ensure they can track and mitigate emerging threats. Review system configurations for misconfigurations and security weaknesses. Implementing a robust configuration and patch management program hinders sophisticated APT operations by limiting the effectiveness of opportunistic attacks.

2. **Disable unnecessary ports, protocols, and services.** Review network security device logs and determine whether to shut off unnecessary ports and protocols. Monitor common ports and protocols for C2 activity. Turn off or disable any unnecessary services or functionality within devices (e.g., universal plug and play [UPnP], PowerShell).

3. **Enhance monitoring of network and email traffic.** Review network signatures and indicators for focused operations activities, monitor for new phishing themes, and adjust email rules accordingly. Follow best practices of restricting attachments via email. Ensure that log information is aggregated and correlated to enable maximum detection capabilities, with a focus on monitoring for account misuse.

4. **Use protection capabilities to stop malicious activity.** Implement antivirus software and other endpoint protection capabilities to automatically detect and prevent malicious files from executing. Use network intrusion detection and prevention systems to identify and prevent commonly employed adversarial malware and limit nefarious data transfers.

Contact Information

CISA encourages recipients of this report to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact CISA at:

- 1-888-282-0870 (From outside the United States: +1-703-235-8832)
- Central@cisa.dhs.gov (UNCLASS)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on the CISA homepage at http://www.us-cert.cisa.gov/.

References

Revisions

October 1, 2020: Initial Version

October 20, 2020: Recommended Actions Section Updated

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.