Lab 4.1.1a Research Vulnerabilities

Thursday, July 20, 2023 4:35 PM

Lab 4.1.1a Research Vulnerabilities

-

CVE- # - #:	CVE-2019-19781
CVSS Score:	**9.8**
Severity Level:	**Critical**
Name:	**Citrix ADC, Gateway, and SD-WAN WANOP Appliance Code Execution Vulnerability**
Vulnerability Summary: CVE-2019-19781 is a critical vulnerability in Citrix Application Delivery Controller (ADC) and Citrix Gateway (formerly NetScaler ADC and Gateway). An unauthenticated attacker can exploit this flaw to execute arbitrary code. The vulnerability also affects certain deployments of Citrix SD-WAN WANOP edition, which includes Citrix ADC as a load balancer. Immediate action is required to apply relevant security patches and prevent unauthorized code execution on affected systems.	
Vulnerability Impact: This vulnerability has a "Critical" impact and affects the following supported product versions on all supported platforms: • Citrix ADC and Citrix Gateway version 13.0 all supported builds before 13.0.47.24 • NetScaler ADC and NetScaler Gateway version 12.1 all supported builds before 12.1.55.18 • NetScaler ADC and NetScaler Gateway version 12.0 all supported builds before 12.0.63.13 • NetScaler ADC and NetScaler Gateway version 11.1 all supported builds before 11.1.63.15 • NetScaler ADC and NetScaler Gateway version 10.5 all supported builds before 10.5.70.12 • Citrix SD-WAN WANOP appliance models 4000-WO, 4100-WO, 5000-WO, and 5100-WO all supported software release builds before 10.2.6b and 11.0.3b	
Recommendations: Citrix strongly urges affected customers to immediately upgrade to a fixed build or apply the provided mitigation that also applies to Citrix ADC, Citrix Gateway and Citrix SD-WAN WANOP deploymets. Your can download the fixed builds at https://www.citrix.com/downloads/citrix-adc/ and https://www.citrix.com/downloads/citrix-sd-wan/ . You can also download the Verification Tool upon application mitigation steps to verify correctness here: https://support.citrix.com/article/CTX269180	
References: Citrix Support Knowledge Center: https://support.citrix.com/article/CTX267027/cve201919781-vulnerability-in-citrix-application-delivery-controller-citrix-gateway-and-citrix-sdwan-wanop-appliance NIST National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2019-19781	

CVE- # - #:	CVE-2019-11510
CVSS Score:	**10.0**
Severity Level:	**Critical**
Name:	**Pulse Connect Secure VPN Vulnerability**
Vulnerability Summary: CVE-2019-11510 is a critical arbitrary file disclosure vulnerability in Pulse Connect Secure, the SSL VPN solution from Pulse Secure. The flaw allows remote, unauthenticated attackers to obtain usernames and plaintext passwords from vulnerable endpoints. Despite a patch being released in April 2019, numerous organizations continue to be at risk due to unpatched Pulse Secure VPN servers.	
Vulnerability Impact: This vulnerability has a "Critical" impact. Over 3,800 vulnerable endpoints have been detected, with a significant number residing in the United States. Urgent action is necessary to prevent compromise in potential attacks. Affected Versions: ● Pulse Connect Secure 9.0R1 - 9.0R3.3 ● Pulse Connect Secure 8.3R1 - 8.3R7 ● Pulse Connect Secure 8.2R1 - 8.2R12 ● Pulse Connect Secure 8.1R1 - 8.1R15 ● Pulse Policy Secure 9.0R1 - 9.0R3.1 ● Pulse Policy Secure 5.4R1 - 5.4R7 ● Pulse Policy Secure 5.3R1 - 5.3R12 ● Pulse Policy Secure 5.2R1 - 5.2R12 ● Pulse Policy Secure 5.1R1 - 5.1R15	
Recommendations: The Cybersecurity and Infrastructure Security Agency (CISA) warns of ongoing exploitation and strongly advises users and administrators to promptly update to the provided fixes. Here you can download the updated version: https://forums.ivanti.com/s/welcome-pulse-secure?language=en_US	
References: Tenable Blog: https://www.tenable.com/blog/cve-2019-11510-critical-pulse-connect-secure-vulnerability-used-in-sodinokibi-ransomware Cybersecurity Infrastructure Security Agency: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-010a The MIRTE Corporation CVE Log: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510 Ivanti: https://forums.ivanti.com/s/welcome-pulse-secure?language=en_US	

CVE- # - #:	CVE-2019-0143
CVSS Score:	**5.5**
Severity Level:	**Medium**
Name:	**Intel Ethernet 700 Series Improper Handling of Exceptional Conditions**
Vulnerability Summary: CVE-2019-0143 is a vulnerability affecting Intel(R) Ethernet 700 Series Controllers versions before 7.0. An authenticated local user can exploit this flaw to potentially enable a denial-of-service attack. The vulnerability is caused by improper access restrictions in the firmware, allowing unauthorized access to restricted functionality,	

leading to a DoS condition on the targeted system.	
Vulnerability Impact: The vulnerability is a "medium" impact. It affects Intel(R) Ethernet 700 Series Controllers versions before 7.0 particularly in cloud environments.	
Recommendations: Immediate attention is necessary to apply patches and mitigate potential risks associated with this vulnerability. You can obtain the patches here: https://www.cybersecurity-help.cz/vdb/intel/	
References: Intel: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00255.html National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2019-0143 MyF5: https://my.f5.com/manage/s/article/K08441753	

CVE- # - #:	CVE-2019-8174
CVSS Score:	**8.8**
Severity Level:	**High**
Name:	**Adobe Acrobat and Reader versions vulnerability.**
Vulnerability Summary: CVE-2019-8174 is a critical untrusted pointer dereference vulnerability found in multiple versions of Adobe Acrobat and Reader, including 2019.012.20040 and earlier, 2017.011.30148 and earlier, and 2015.006.30503 and earlier. This flaw could be exploited by an attacker to execute arbitrary code on the affected system.	
Vulnerability Impact: This vulnerability has a "high" impact on the following: • 2019.012.20040 and earlier • 2017.011.30148 and earlier • 2017.011.30148 and earlier • 2015.006.30503 and earlier • 2015.006.30503 and earlier	
Recommendations: It is imperative for users to promptly update their software to the latest versions to prevent potential arbitrary code execution and secure their systems against this vulnerability. Follow solution guide here: https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	
References: National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2019-8174	

Rapid7: https://www.rapid7.com/db/vulnerabilities/acrobat-cve-2019-8174/ Adobe Security Bulletin: https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	