Advisory Alert

Alert Number: AAA20230615 **Date:** June 15, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Citrix	**Critical**	Improper Access control vulnerability
Ivanti	**Critical**	Multiple Cross site scripting Vulnerabilities
ubuntu	**High**, **Medium**	Multiple Vulnerabilities
ivanti	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Palo Alto	**Medium**	Multiple Vulnerabilities
Citrix	**Medium**	Improper Access control vulnerability
Dell	**Medium**	Multiple Improper Input Validation Vulnerabilities

Description

Affected Product	**Citrix**
Severity	Critical
Affected Vulnerability	Improper Access control vulnerability (CVE-2023-24489)
Description	Citrix has released a security update addressing Access control vulnerability.if exploited Remote unauthenticated attacker can compromise the customer-managed ShareFile storage zones controller. Citrix highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Customer-managed ShareFile storage zones controller before version 5.11.24.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX559517/sharefile-storagezones-controller-security-update-for-cve202324489

Affected Product	**Ivanti**
Severity	Critical
Affected Vulnerability	Multiple Cross site scripting Vulnerabilities (CVE-2016-4789, CVE-2016-4790)
Description	Ivanti has released security updates addressing Multiple Cross site scripting Vulnerabilities in Pulse Connect Secure devices. These Vulnerabilities exists in a file that is located in the authenticated area and system configuration section of the administrative user interface. Ivanti highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Pulse Connect Secure versions 8.2r1, 8.1r2, 8.0r9, and 7.4r13.4.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/SA40209?language=en_US https://forums.ivanti.com/s/article/SA40211?language=en_US

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31436, CVE-2023-2612, CVE-2023-30456, CVE-2023-1380 CVE-2023-32233)
Description	Ubuntu has released a security update addressing multiple vulnerabilities in Ubuntu 20.04. If exploited these vulnerabilities could cause arbitrary Code execution, sensitive information disclosure and Denial of Service. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6162-1

Affected Product	**Ivanti**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2014-3566, CVE-2016-4786, CVE-2016-4787, CVE-2016-4791 CVE-2016-4792, CVE-2016-4788)
Description	Ivanti has released security updates addressing multiple vulnerabilities in Pulse Connect Secure and Pulse Policy Secure. If exploited these vulnerabilities could cause information disclosure and Denial of Service. Ivanti recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Pulse Connect Secure versions before 8.2r1, 8.1r2, 8.0r10, 7.4r13.4. , 8.0r11, 8.0r9 Pulse Policy Secure
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/JSA10656?language=en_US https://forums.ivanti.com/s/article/SA40206?language=en_US https://forums.ivanti.com/s/article/SA40207?language=en_US https://forums.ivanti.com/s/article/SA40210?language=en_US https://forums.ivanti.com/s/article/SA40212?language=en_US https://forums.ivanti.com/s/article/SA40208?language=en_US

Affected Product	**Palo Alto**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0009, CVE-2023-0010)
Description	Palo Alto has released security updates addressing multiple vulnerabilities in PAN-OS and GlobalProtect App. If exploited these vulnerabilities could cause Reflected Cross-Site Scripting and Local Privilege Escalation. **CVE-2023-0009-** A local privilege escalation vulnerability in the GlobalProtect app on Windows enables a local service account or user with token impersonation privileges to execute programs with elevated privileges. **CVE-2023-0010-** A reflected cross-site scripting vulnerability in the Captive Portal feature of PAN-OS software can allow a JavaScript payload to be executed in the context of an authenticated Captive Portal user's browser when they click on a specifically crafted link. Palo Alto recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	GlobalProtect App 6.1 versions before 6.1.1 on Windows GlobalProtect App 6.0 versions before 6.0.5 on Windows GlobalProtect App 5.2 versions before 5.2.13 on Windows PAN-OS 10.2 versions before 10.2.2 PAN-OS 10.1 versions before 10.1.6 PAN-OS 10.0 versions before 10.0.11 PAN-OS 9.1 versions before 9.1.16 PAN-OS 9.0 versions before 9.0.17 PAN-OS 8.1 versions before 8.1.24
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2023-0009 https://security.paloaltonetworks.com/CVE-2023-0010

Affected Product	**Citrix**
Severity	**Medium**
Affected Vulnerability	Improper Access control vulnerability (CVE-2023-24490)
Description	Citrix has released a security update addressing Access control vulnerability. If exploited Authorized Users with only access to launch Virtual Delivery Agents applications can launch an unauthorized desktop. Citrix recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Citrix Virtual Apps and Desktops versions before 2305 Citrix Virtual Apps and Desktops 2203 LTSR before CU3 Citrix Virtual Apps and Desktops 1912 LTSR before CU7 Linux Virtual Delivery Agent versions before 2305 Linux Virtual Delivery Agent 2203 LTSR before CU3 Linux Virtual Delivery Agent 1912 LTSR before CU7 hotfix 1(19.12.7001)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX559370/windows-and-linux-virtual-delivery-agent-for-cvad-and-citrix-daas-security-bulletin-cve202324490

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Improper Input Validation Vulnerabilities (CVE-2023-25936, CVE-2023-25937, CVE-2023-25938, CVE-2023-28026, CVE-2023-28027, CVE-2023-28028, CVE-2023-28029, CVE-2023-28030, CVE-2023-28031, CVE-2023-28032, CVE-2023-28033, CVE-2023-28034, CVE-2023-28035, CVE-2023-28036, CVE-2023-28039, CVE-2023-28040, CVE-2023-28041, CVE-2023-28042, CVE-2023-28044, CVE-2023-28050, CVE-2023-28052, CVE-2023-28054, CVE-2023-28058, CVE-2023-28059, CVE-2023-28060, CVE-2023-28061)
Description	Dell has released a security update addressing Multiple Improper Input Validation Vulnerabilities in Dell BIOS. This vulnerability could allow a local authenticated malicious user with administrator privileges to modify a UEFI variable. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000212204/dsa-2023-099-dell-client-bios-security-update-for-multiple-improper-input-validation-vulnerabilities

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.