Advisory Alert

Alert Number: AAA20250311 **Date:** March 11, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	OS command injection Vulnerability
Zyxel	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
HPE	**High**, Medium	Multiple Signature Verification Vulnerabilities
Ivanti	Medium	Path Traversal Vulnerability

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	OS Command Injection Vulnerability (CVE-2024-47908)
Description	Ivanti has released a security update addressing an OS Command injection Vulnerability that exists in Cloud Services Application (CSA). **CVE-2024-47908** - OS command injection in the admin web console of Ivanti CSA before version 5.0.5 allows a remote authenticated attacker with admin privileges to achieve remote code execution. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti CSA - 5.0.4 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Services-Application-CSA-CVE-2024-47908-CVE-2024-11771?language=en_US

Affected Product	**Zyxel**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-11253, CVE-2024-12009, CVE-2024-12010)
Description	Zyxel has released patches for certain DSL/Ethernet CPE, fiber ONT, and WiFi extender firmware versions affected by post-authentication command injection vulnerabilities. **CVE-2024-11253 -** The post-authentication command injection vulnerability in the "DNSServer" parameter of the diagnostic function in certain DSL/Ethernet CPE firmware versions could allow an authenticated attacker with administrator privileges to execute operating system (OS) commands on a vulnerable device. It is important to note that WAN access is disabled by default on these devices, and this attack can only be successful if the strong, unique administrator passwords have been compromised. **CVE-2024-12009 -** The post-authentication command injection vulnerability in the "ZyEE" function of certain DSL/Ethernet CPE, fiber ONT, and WiFi extender firmware versions could allow an authenticated attacker with administrator privileges to execute OS commands on a vulnerable device. It is important to note that WAN access is disabled by default on these devices, and this attack can only be successful if the strong, unique administrator passwords have been compromised. **CVE-2024-12010 -** The post-authentication command injection vulnerability in the ”zyUtilMailSend” function of certain DSL/Ethernet CPE, fiber ONT, and WiFi extender firmware versions could allow an authenticated attacker with administrator privileges to execute OS commands on a vulnerable device. It is important to note that WAN access is disabled by default on these devices, and this attack can only be successful if the strong, unique administrator passwords have been compromised. Zyxel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-vulnerabilities-in-certain-dsl-ethernet-cpe-fiber-ont-and-wifi-extender-devices-03-11-2025

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34195, CVE-2023-20555)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-34195 -** Dell Client Platform INSYDE UEFI BIOS remediation is available for an arbitrary code execution vulnerability that could be exploited by malicious users to compromise the affected system. **CVE-2023-20555 -** AMD BIOS remediation is available for an SMM Corruption Vulnerability that could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000217234/dsa-2023-325-security-update-for-dell-client-platform-insyde-uefi-bios-vulnerability • https://www.dell.com/support/kbdoc/en-us/000216230/dsa-2023-177-security-update-for-an-amd-bios-vulnerability

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Signature Verification Vulnerabilities (CVE-2024-56161, CVE-2024-36347)
Description	HPE has released security updates addressing Multiple Signature Verification Vulnerabilities that exist in their products. **CVE-2024-36347** - A potential security vulnerability has been identified in certain HPE ProLiant DL/XL Servers. Improper signature verification in AMD CPU ROM microcode patch loader may allow an attacker with local administrator privilege to load malicious microcode, potentially resulting in loss of integrity of x86 instruction execution, loss of confidentiality and integrity of data in x86 CPU privileged context and compromise of SMM execution environment. **CVE-2024-56161 -** Improper signature verification in AMD CPU ROM microcode patch loader may allow an attacker with local administrator privilege to load malicious CPU microcode resulting in loss of confidentiality and integrity of a confidential guest running under AMD SEV-SNP. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• HPE ProLiant DL145 Gen11 - Prior to v1.40_01-17-2025 • HPE ProLiant DL325 Gen11 Server - Prior to v2.30_01-17-2025 • HPE ProLiant DL365 Gen11 Server - Prior to v2.30_01-17-2025 • HPE ProLiant DL385 Gen11 Server - Prior to v2.30_01-17-2025 • HPE ProLiant DL325 Gen10 Plus server - Prior to v3.60_01-16-2025 • HPE ProLiant DL325 Gen10 Plus v2 server - Prior to v3.60_01-16-2025 • HPE ProLiant DL365 Gen10 Plus server - Prior to v3.60_01-16-2025 • HPE ProLiant DL385 Gen10 Plus server - Prior to v3.60_01-16-2025 • HPE ProLiant DL385 Gen10 Plus v2 server - Prior to v3.60_01-16-2025 • HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to v3.60_01-16-2025 • HPE ProLiant DL325 Gen10 Server - Prior to v3.40_01-16-2025 • HPE ProLiant DL385 Gen10 Server - Prior to v3.40_01-16-2025
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04826en_us&docLocale=en_US

Affected Product	**Ivanti**
Severity	**Medium**
Affected Vulnerability	Path Traversal Vulnerability (CVE-2024-11771)
Description	Ivanti has released security updates addressing a Path Traversal Vulnerability that exists in Cloud Service Application (CSA) Platform. **CVE-2024-11771 -** Path traversal in Ivanti CSA before version 5.0.5 allows a remote unauthenticated attacker to access restricted functionality. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti CSA - 5.0.4 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Services-Application-CSA-CVE-2024-47908-CVE-2024-11771?language=en_US

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.