Advisory Alert

Alert Number: AAA20250416 **Date:** April 16, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Stack-based Buffer Overflow Vulnerability
HPE	**Critical**	Buffer Overflow Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Oracle	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
FortiGuard	**High**	Multiple Improper Access Control Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Oracle	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
F5	**Low**	Denial Of Service Vulnerability
SolarWinds	**Low**	Client-Side Cross-Site Scripting Vulnerability

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Stack-based Buffer Overflow Vulnerability (CVE-2025-22457)
Description	Ivanti has released security updates addressing a Stack-based Buffer Overflow Vulnerability that exists in Ivanti Connect. Successful exploitation allows a remote unauthenticated attacker to achieve remote code execution. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Connect Secure 22.7R2.5 and prior Pulse Connect Secure (EoS) 9.1R18.9 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2020-10188)
Description	HPE has released security updates addressing a Buffer Overflow Vulnerability that exists in HP-UX Telnetd. Due to a remote buffer overflow involving the netclear and nextitem functions, HP-UX telnetd allows remote attackers to execute arbitrary code via short writes or urgent data. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HP-UX 11.31 PHNE_42509
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbux04206en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Precision Rack and VxRail Appliance firmware. These vulnerabilities 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	Dell VxRail Appliance Versions prior to 8.0.311 Dell EMC VxRail Appliance 8.0.x versions prior to 8.0.300 Precision 7920 Rack iDRAC9 firmware Versions prior to 7.00.00.181 Precision 7920 XL Rack iDRAC9 firmware Versions prior to 7.00.00.181
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000245873/dsa-2024-431-security-update-for-dell-vxrail-8-0-311-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000227832/dsa-2024-341-security-update-for-dell-vxrail-8-0-300-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000306810/dsa-2025-179 • https://www.dell.com/support/kbdoc/en-us/000226863/dsa-2024-289-security-update-for-dell-vxrail-8-0-213-multiple-third-party-component-vulnerabilities

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-30707, CVE-2025-30708, CVE-2025-30737, CVE-2025-30716, CVE-2025-30717, CVE-2025-30694, CVE-2025-30730, CVE-2025-30731, CVE-2025-30732, CVE-2025-21587, CVE-2025-21576, CVE-2025-30722, CVE-2025-30692, CVE-2025-30709, CVE-2025-30733, CVE-2025-30712, CVE-2025-30713, CVE-2025-21586, CVE-2025-30740, CVE-2025-30726, CVE-2025-30727, CVE-2025-30728, CVE-2025-30714, CVE-2025-30723, CVE-2025-30724, CVE-2025-30706, CVE-2025-30681, CVE-2025-30682, CVE-2025-30683, CVE-2025-30684, CVE-2025-30685, CVE-2025-30687, CVE-2025-30688, CVE-2025-30701, CVE-2025-30718, CVE-2025-30711, CVE-2025-30719, CVE-2025-30725)
Description	Oracle has released monthly critical Patch updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Oracle 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.oracle.com/security-alerts/cpuapr2025.html

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-32487, CVE-2020-36242, CVE-2023-28154, CVE-2019-9021, CVE-2023-51714, CVE-2019-20478, CVE-2019-9641, CVE-2018-20505, CVE-2019-9023, CVE-2019-9020, CVE-2018-20506, CVE-2019-9639, CVE-2019-9638, CVE-2018-20346, CVE-2018-1311, CVE-2023-51385)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in QRadar. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution, Security Restrictions Bypass, Denial of Service and use-after-free conditions. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar EDR v3.12 IBM QRadar SIEM versions 7.5 - 7.5.0 UP9 QRadar Incident Forensics versions 7.5 - 7.5.0 UP9 IF03 IBM QRadar Use Case Manager app versions 1.0.0 - 3.10.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7182424 • https://www.ibm.com/support/pages/node/7162077 • https://www.ibm.com/support/pages/node/7145367 • https://www.ibm.com/support/pages/node/7173420 • https://www.ibm.com/support/pages/node/7148094 • https://www.ibm.com/support/pages/node/7174634

Affected Product	**FortiGuard**
Severity	**High**
Affected Vulnerability	Multiple Improper Access Control Vulnerabilities (CVE-2024-26013, CVE-2024-50565)
Description	FortiGuard has released security updates addressing multiple Improper Access Control Vulnerabilities that exist in their products. **CVE-2024-26013/ CVE-2024-50565** - An improper restriction of communication channel to intended endpoints vulnerability in multiple Fortinet products may allow an unauthenticated attacker in a man-in-the-middle position to impersonate the management device, via intercepting the FGFM authentication request between the management device and the managed device. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiAnalyzer 7.4 versions 7.4.0 through 7.4.2 FortiAnalyzer 7.2 versions 7.2.0 through 7.2.4 FortiAnalyzer 7.0 versions 7.0.0 through 7.0.11 FortiAnalyzer 6.4 versions 6.4.0 through 6.4.14 FortiAnalyzer 6.2 versions 6.2.0 through 6.2.13 FortiManager 7.4 versions 7.4.0 through 7.4.2 FortiManager 7.2 versions 7.2.0 through 7.2.4 FortiManager 7.0 versions 7.0.0 through 7.0.11 FortiManager 6.4 versions 6.4.0 through 6.4.14 FortiManager 6.2 versions 6.2.0 through 6.2.13 FortiOS 7.4 versions 7.4.0 through 7.4.4 FortiOS 7.2 versions 7.2.0 through 7.2.8 FortiOS 7.0 versions 7.0.0 through 7.0.15 FortiOS 6.4 all versions FortiOS 6.2 versions 6.2.0 through 6.2.16 FortiProxy 7.4 versions 7.4.0 through 7.4.2 FortiProxy 7.2 versions 7.2.0 through 7.2.9 FortiProxy 7.0 versions 7.0.0 through 7.0.15 FortiProxy 2.0 all versions FortiVoice 7.0 versions 7.0.0 through 7.0.2 FortiVoice 6.4 versions 6.4.0 through 6.4.8 FortiVoice 6.0 all versions FortiWeb 7.4 versions 7.4.0 through 7.4.2 FortiWeb 7.2 all versions FortiWeb 7.0 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-046

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE 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.suse.com/support/update/

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Red Hat 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://access.redhat.com/security/security-updates/security-advisories?q=&p=1&sort=portal_publication_date+desc&rows=100&portal_advisory_type=Security+Advisory&documentKind=Errata

Affected Product	**Oracle**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released security updates addressing multiple vulnerabilities that exist in Oracle Linux and Oracle Solaris Third Party products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Solaris 11.4, 11.3 and 10 Oracle Linux 8 and 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.oracle.com/security-alerts/bulletinapr2025.html • https://www.oracle.com/security-alerts/linuxbulletinapr2025.html

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in QRadar. These vulnerabilities could be exploited by malicious users to cause Server-side Request Forgery, Arbitrary Command Execution, Denial Of Service, Information Disclosure, Privilege Escalation. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP10 IBM QRadar Incident Forensics versions 7.5 - 7.5.0 UP9 IF03 IBM QRadar Use Case Manager App versions 1.0.0 - 3.10.0 IBM QRadar Data Synchronization App versions 1.0 - 3.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7162077 • https://www.ibm.com/support/pages/node/7150684 • https://www.ibm.com/support/pages/node/7145367 • https://www.ibm.com/support/pages/node/7173420 • https://www.ibm.com/support/pages/node/7148094 • https://www.ibm.com/support/pages/node/7177981 • https://www.ibm.com/support/pages/node/7184092 • https://www.ibm.com/support/pages/node/7174634 • https://www.ibm.com/support/pages/node/7150684

Affected Product	**F5**
Severity	**Low**
Affected Vulnerability	Denial Of Service Vulnerability (CVE-2024-11187)
Description	F5 has released security updates addressing a Denial Of Service Vulnerability that exists in BIG-IP modules. **CVE-2024-11187** - It is possible to construct a zone such that some queries to it will generate responses containing numerous records in the Additional section. An attacker sending DNS queries that can cause either the authoritative server itself or an independent resolver to use disproportionate resources processing the queries. This may ultimately result in the server not being able to attend new requests and leading to a denial of service. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) versions 17.5.0, 17.1.0 - 17.1.2, 16.1.0 - 16.1.5, 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000150814

Affected Product	**SolarWinds**
Severity	**Low**
Affected Vulnerability	Client-Side Cross-Site Scripting Vulnerability (CVE-2024-45712)
Description	SolarWinds has released security updates addressing a Client-Side Cross-Site Scripting Vulnerability that exists in Serv-U. **CVE-2024-45712** - SolarWinds Serv-U is vulnerable to a client-side cross-site scripting (XSS) vulnerability. The vulnerability can only be performed by an authenticated account, on the local machine, from the local browser session. Therefore the risk is very low. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Serv-U 15.5 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2024-45712

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.