Advisory Alert

Alert Number: **AAA20260130** **Date:** **January 30, 2026**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Code Injection Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
WatchGuard	**High**	LDAP Injection vulnerability
Dell	**High, Medium**	Multiple Vulnerabilities
Ubuntu	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Code Injection Vulnerabilities (CVE-2026-1281, CVE-2026-1340)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their Endpoint Manager Mobile (EPMM) products. **CVE-2026-1281-** A code injection vulnerability where an unauthenticated remote attacker can send a specially crafted request to trigger arbitrary code execution (remote code execution, RCE) in Ivanti EPMM due to improper code generation control. **CVE-2026-1340 -** Another critical code injection flaw in Ivanti EPMM with similar exploitation that allows remote, unauthenticated arbitrary code execution. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager Mobile (EPMM) • 12.5.0.0 and prior • 12.6.0.0 and prior • 12.7.0.0 and prior • 12.5.1.0 and prior • 12.6.1.0 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-39898, CVE-2025-39971, CVE-2025-40248)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel of their products. **CVE-2025-39898 -** A heap overflow exists in the Linux kernel's e1000e network driver due to insufficient input validation in the e1000_set_eeprom function, which can cause memory corruption and crashes or other impacts if exploited. **CVE-2025-39971 -** A flaw in the i40e Ethernet driver for Intel hardware, where improper index validation in configuration queue messages could lead to incorrect processing or memory issues, potentially impacting stability or security. **CVE-2025-40248 -** A vulnerability in the Linux kernel's vsock subsystem where a use-after-free/memory corruption issue may occur, potentially allowing local attackers to cause system instability or escalate privileges. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 x86_64 • Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x • Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64 • Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:1581

Affected Product	**WatchGuard**
Severity	**High**
Affected Vulnerability	LDAP Injection vulnerability (CVE-2026-1498)
Description	WatchGuard has released security updates addressing a vulnerability that exists in their Firebox products. **CVE-2026-1498 -** An LDAP Injection vulnerability in WatchGuard Fireware OS may allow a remote unauthenticated attacker to extract sensitive information from a connected LDAP authentication server via an exposed authentication or management web interface. Under certain conditions, an attacker could also authenticate as an LDAP user if they possess the user's passphrase. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Fireware OS 12.5.x (prior to 12.5.16) • T15, T35 Fireware OS 2025.1.x (prior to 2026.1) • T115-W, T125, T125-W, T145, T145-W, T185, M295, M395, M495, M595, M695 Fireware OS 12.x (prior to 12.11.7) • T20, T25, T40, T45, T55, T70, T80, T85, M270, M290, M370, M390, M470, M570, M590, M670, M690, M440, M4600, M4800, M5600, M5800, Firebox Cloud, Firebox NV5, FireboxV
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00001

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-28005, CVE-2023-2650, CVE-2023-3817, CVE-2023-5678, CVE-2024-47875, CVE-2025-22398, CVE-2025-24381, CVE-2025-24382, CVE-2025-24383)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their Products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell SD-WAN EDGE620/640/680 - Versions prior to 3.50.0.9-21 Dell SD-WAN EDGE610/610-LTE - Versions prior to 3.43.0.9-24 Dell EMC Networking VEP1425/VEP1445/VEP1485 - Versions prior to 2.6 Dell Networking VEP4600 - Versions prior to 4.3 PowerSwitch E3200-ON Series - Versions prior to 3.57.5.1-5 PowerSwitch S5448F-ON - Versions prior to 3.52.5.1-12 PowerSwitch N2200-ON Series - Versions prior to 3.45.5.1-31 PowerSwitch N3200-ON Series - Versions prior to 3.45.5.1-31 PowerSwitch Z9264F-ON - Versions prior to 3.42.5.1-21 PowerSwitch Z9432F-ON - Versions prior to 3.51.5.1-21 PowerSwitch Z9664F-ON - Versions prior to 3.54.5.1-9 Dell Unity (Dell Unity Operating Environment (OE) - Versions prior to 5.5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000421209/dsa-2026-067-security-update-for-dell-networking-products-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000421244/dsa-2026-068-security-update-for-dell-networking-products-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000421197/dsa-2026-054-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-39993, CVE-2024-56756, CVE-2024-56606, CVE-2024-50195, CVE-2024-49959, CVE-2024-27078, CVE-2022-48986, CVE-2024-53164, CVE-2021-47485, CVE-2025-38352, CVE-2024-57850, CVE-2024-53197, CVE-2024-26689)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their Products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu Versions 14.04, 16.04, 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7988-1 • https://ubuntu.com/security/notices/USN-7987-1 • https://ubuntu.com/security/notices/USN-7986-1

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their Products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 versions 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/bulletin/

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.