Advisory Alert

Alert Number: AAA20260907 **Date:** September 7, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
ASUS	**Critical**	Security Update
Red Hat	**High**	Multiple Vulnerabilities
Zyxel Networks	**High**, **Medium**	Multiple Vulnerabilities
MongoDB	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Hitachi	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**Medium**	Local Disclosure of Information Vulnerability

Description

Vendor	**ASUS**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2026-75754)
Description	ASUS has released a security update addressing a vulnerability that exists in their product. **CVE-2026-75754:** Missing Authentication for Critical Function, Server-Side Request Forgery (SSRF), and Use of Hard-coded Credentials in ASUS Control Center allow an unauthorized user to obtain the encryption key via an HTTP request, causing a local service to enable SSH on port 2222. The attacker can then log in with the hardcode credentials to obtain a root shell, enabling direct reading, writing, and deletion of data on ASUS Control Center, as well as remote control of all servers, PCs, and workstations ASUS advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ASUS Control Center Enterprise (ACC) 4.0.0.2 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-74582, CVE-2026-74480)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-74582:** A flaw was found in the Linux kernel's packet handling functions, specifically packet_snd() and packet_sendmsg_spkt(). This vulnerability arises from inconsistent handling of network device header lengths during packet construction. A local attacker could exploit this by triggering a race condition during device reconfiguration, leading to an out-of-bounds write. This could potentially allow for privilege escalation or arbitrary code execution. **CVE-2026-74480:** A flaw was found in the Linux kernel's network bridge module. When handling multicast fast-leave, a vulnerability exists where the system may attempt to access a port group after it has been deleted. This can occur if multicast-to-unicast was previously enabled and then disabled, leading to a stale pointer. This memory corruption vulnerability could lead to system instability or a denial of service. 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 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle Long Life 8.8 x86_64 Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:63537 • https://access.redhat.com/errata/RHSA-2026:63538

Vendor	**Zyxel Networks**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-6837, CVE-2026-8508, CVE-2026-14818)
Description	Zyxel Networks has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-6837:** A post-authentication command injection vulnerability in the "export-cgi" CGI program in certain AP firmware versions could allow an authenticated attacker with administrator privileges to execute OS commands on an affected device. **CVE-2026-8508:** An improper authentication vulnerability in the "social_login.cgi" CGI program in certain firmware versions of APs, FWA7, and Security Routers could allow an attacker on the WLAN to bypass captive portal authentication. **CVE-2026-14818:** A path traversal vulnerability in the CLI command used to execute configuration files in certain versions of ZLD firewall firmware could allow an authenticated attacker with administrator privileges to execute a crafted malicious configuration file on an affected device. Zyxel Networks 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-command-injection-and-improper-authentication-vulnerabilities-in-certain-aps-fwa7-and-security-routers-08-04-2026 • https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-path-traversal-vulnerability-in-the-configuration-file-execution-cli-command-of-zld-firewalls-08-04-2026

Vendor	**MongoDB**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-84968, CVE-2026-84967, CVE-2026-84962, CVE-2026-84963, CVE-2026-84964, CVE-2026-84965, CVE-2026-84966, CVE-2026-84969, CVE-2026-84971, CVE-2026-84970)
Description	MongoDB has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MongoDB for VS Code - 1.13.0 affects versions prior to 1.17.1 libmongocrypt - affects versions prior to 1.20.2 C++ Driver - 3.2.0 affects versions prior to 4.5.2 PHP Driver • 1.15.0 affects versions prior to 1.21.8 • 2.0.0 affects versions prior to 2.5.1 C Driver • 1.10.0 affects versions prior to 1.30.9 • 2.0.0 affects versions prior to 2.5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

Vendor	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53309, CVE-2026-53246, CVE-2026-53225, CVE-2026-53224, CVE-2026-53043, CVE-2026-53045, CVE-2026-53002, CVE-2026-52914, CVE-2026-43071, CVE-2022-50401)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 14.04, 16,04, 18.04, 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8714-2 • https://ubuntu.com/security/notices/USN-8725-1

Vendor	**Hitachi**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Hitachi has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Hitachi advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H Hitachi Virtual Storage Platform 5100, 5500, 5100H, 5500H
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/06.html

Vendor	**HPE**
Severity	**Medium**
Affected Vulnerability	Local Disclosure of Information Vulnerability (CVE-2026-20917)
Description	HPE has released a security update addressing a vulnerability that exist in their products. **CVE-2026-20917:** Exposure of sensitive information caused by incorrect data forwarding during transient execution for some Intel(R) Processors within Ring 0: Hypervisor and Kernel may allow information disclosure. System software adversary with a privileged user combined with a high complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE StoreEasy 1660 Storage - Prior to 2.70_08-19-2026 HPE StoreEasy 1860 Storage - Prior to 2.70_08-19-2026 HPE StoreEasy 1670 Expanded Storage - Prior to 2.70_08-19-2026
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05128en_us&docLocale=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.