Advisory Alert

Alert Number: AAA20260312 **Date:** March 12, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**High**	Access Bypass Vulnerability
Hitachi	**High**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
ASUS	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Access Bypass Vulnerability
Description	Drupal has released a security update addressing a vulnerability that exists in their products. This vulnerability could be exploited by malicious users to conduct Authentication Bypass Attacks. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Unpublished Node Permissions module versions prior to 1.7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-029

Affected Product	**Hitachi**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-7386, CVE-2023-37364)
Description	Hitachi has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-7386**: When external authentication is used, this vulnerability that may expose authentication-related information. The data stored in the Hitachi disk array system will not be accessed. **CVE-2023-37364**: In WS-Inc J WBEM Server 4.7.4 before 4.7.5, the CIM-XML protocol adapter does not disable entity resolution. This allows context-dependent attackers to read arbitrary files or cause a denial of service. Hitachi advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Virtual Storage Platform G Series: • G100, G130, G150, G200, G350, G370, G400, G600, G700, G800, G900, G1000, G1500 Virtual Storage Platform F Series: • F350, F370, F400, F600, F700, F800, F900, F1500 Virtual Storage Platform 5000 Series: • 5100, 5100H, 5200, 5200H, 5500, 5500H, 5600, 5600H Virtual Storage Platform VX Series: • VX7, VX8 Virtual Storage Platform E Series: • E590, E590H, E790, E790H, E990, E1090, E1090H
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/2026_301.html • https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/2026_303.html#vuln

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20118, CVE-2026-20074, CVE-2026-20040, CVE-2026-20046, CVE-2026-20116, CVE-2026-20117)
Description	Cisco 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. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Cisco IOS XR versions: • 7.8 to 7.11 • 24.1 to 24.4 • 25.1 to 25.3 Cisco Unified Intelligence Center versions: • 12.6 and earlier • 15.0 Cisco Finesse versions: • 12.6 and earlier • 15.0 Cisco Unified CCX Release versions: • 12.5 SU3 and earlier • 15.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xrncs-epni-int-dos-TWMffUsN • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-isis-dos-kDMxpSzK • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-privesc-bF8D5U4W • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cc-xss-MrNAH5Jh

Affected Product	**ASUS**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-15037, CVE-2025-15038)
Description	ASUS has released security updates addressing multiple vulnerabilities that exist in the ASUS Business Control Interface. **CVE-2025-15037**: An Incorrect Permission Assignment vulnerability exists in the ASUS Business System Control Interface driver. This vulnerability can be triggered by an unprivileged local user sending a specially crafted IOCTL request, potentially leading to unauthorized access to sensitive hardware resources and kernel information disclosure. **CVE-2025-15038**: An Out-of-Bounds Read vulnerability exists in the ASUS Business System Control Interface driver. This vulnerability can be triggered by an unprivileged local user sending a specially crafted IOCTL request, potentially leading to a disclosure of kernel information or a system crash. ASUS advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	**ASUS Commercial Devices:** PM3406CKA, PM3606CKA, B3405CCA, B5405CCA, B5605CCA, B3405CVA, B3605CVA, B5405CVA, B5605CVA, P3405CVA, P3605CVA, BR1204FTA, BR1204CTA, BR1104FTA, B3605CCA, BR1104CTA, B1403CVA, B1503CVA, P1403CVA, P1503CVA, B1403CTA, B1503CTA, BM1503CDA, BM1403CDA, P5405CSA, B9403CVAR, B3402FVA, BR1204FGA, BR1204CGA, BR1104FGA, BR1104CGA, B5604CVA, B5604CVF, B5404CVA, B5404CVF, B5404CMA, B5604CMA, B3404CVA, B3404CVF, B3604CVA, B3604CVF, B3404CMA, B3604CMA, L5404CHA, PM700MK, PM700SK, P500SV, V500SV, D501SER, D701SER, D501MER, D701MER, D900MF, D900SF, D700MF, D700SF, V500MV, P500MV, D700MER, D500MER, D700SER, D500SER, D700TER, D500TER, S501MER, S502MER, S701TER, D901MDR, D901SDR, T500MV, T501MV, T701MF, G700TF, GM700TZ, G13CHR, G16CHR, G22CH(14th), PM640KA, PM670KA, P440VA, P470VA, A3202WVA, A3402WVA, A5402WVAR, A5702WVAR
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

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.