Advisory Alert

Alert Number: AAA20260916 **Date:** September 16, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
Oracle	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities
Oracle	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
NGINX	**Medium**	NGINX ngx_http_v3_Module Vulnerability

Description

Vendor	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76670, CVE-2026-76669, CVE-2026-76672, CVE-2026-76673, CVE-2026-76674, CVE-2026-76675)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE Networking EdgeConnect SD-WAN Gateways • ECOS 9.7.x.x: 9.7.0.0 and below • ECOS 9.6.x.x: 9.6.3.1 and below • ECOS 9.5.x.x: 9.5.8.1 and below • ECOS 9.4.x.x: 9.4.8.2 and below HPE Networking EdgeConnect SD-WAN Orchestrator: • Orchestrator 9.7.x: 9.7.0 and below • Orchestrator 9.6.x: 9.6.3 and below • Orchestrator 9.5.x: 9.5.8 and below • Orchestrator 9.4.x: 9.4.10 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05135en_us&docLocale=en_US

Vendor	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-83149, CVE-2026-44024, CVE-2026-17544, CVE-2026-71290, CVE-2026-73194, CVE-2026-83327, CVE-2026-83452, CVE-2026-83462, CVE-2026-41635, CVE-2026-83355, CVE-2026-2332, CVE-2026-71133, CVE-2026-83099, CVE-2026-83059, CVE-2026-83020, CVE-2026-83021, CVE-2026-71163, CVE-2026-73945, CVE-2026-83055, CVE-2026-83056, CVE-2026-83057, CVE-2026-83058, CVE-2026-73948, CVE-2026-83039, CVE-2026-83031, CVE-2026-83038, CVE-2026-82999, CVE-2026-82997, CVE-2026-82998, CVE-2026-73950, CVE-2026-73947, CVE-2026-73940, CVE-2026-47065, CVE-2026-83232, CVE-2026-83094, CVE-2026-83098, CVE-2026-83100, CVE-2026-83108, CVE-2026-70913, CVE-2026-83042, CVE-2026-83054, CVE-2026-83060, CVE-2026-83061, CVE-2026-83062, CVE-2026-83066, CVE-2026-73961, CVE-2026-82994, CVE-2026-82995, CVE-2026-83339, CVE-2026-73956, CVE-2026-73953, CVE-2026-73963, CVE-2026-83035, CVE-2026-83036, CVE-2026-83037, CVE-2026-70756, CVE-2026-70757, CVE-2026-70748, CVE-2026-83000, CVE-2026-83151, CVE-2026-73962, CVE-2026-83029, CVE-2026-83043, CVE-2026-83040, CVE-2026-83027, CVE-2026-73957, CVE-2026-73944, CVE-2026-73946, CVE-2026-83001, CVE-2026-83103, CVE-2026-83107, CVE-2026-83104, CVE-2026-83006, CVE-2026-73952, CVE-2026-83064, CVE-2026-83105, CVE-2026-83282, CVE-2026-83269, CVE-2026-83283, CVE-2026-83268, CVE-2026-87230, CVE-2026-87172, CVE-2026-87188, CVE-2026-87184, CVE-2026-87186, CVE-2026-87128, CVE-2026-87129, CVE-2026-87170, CVE-2026-87214, CVE-2026-87217, CVE-2026-87223, CVE-2026-87189, CVE-2026-87173, CVE-2026-87175, CVE-2026-87176, CVE-2026-83197, CVE-2026-83196, CVE-2026-83201, CVE-2026-83202, CVE-2026-83229, CVE-2026-83154, CVE-2026-83261, CVE-2026-83260)
Description	Oracle 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. Oracle advises to apply these security fixes at your earliest to protect your 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/cspusep2026.html

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43114, CVE-2026-45998, CVE-2026-46054, CVE-2026-46056, CVE-2026-53006, CVE-2026-53016, CVE-2026-53071, CVE-2026-53196, CVE-2026-63886, CVE-2026-64304, CVE-2026-49362, CVE-2026-54515, CVE-2026-57967, CVE-2026-59889, CVE-2026-49364, CVE-2026-8286, CVE-2026-9547, CVE-2026-11721, CVE-2026-11824, CVE-2026-13204, CVE-2026-15816, CVE-2026-43133, CVE-2026-55973, CVE-2026-58014, CVE-2026-58015, CVE-2026-72693, CVE-2026-33818, CVE-2026-39822, CVE-2026-42504, CVE-2026-56858, CVE-2026-56859, CVE-2026-56860, CVE-2026-56862, CVE-2026-33814, CVE-2026-39821, CVE-2025-40149, CVE-2025-68745, CVE-2026-23466, CVE-2026-31479, CVE-2026-31539, CVE-2026-31566, CVE-2026-31656, CVE-2026-31663, CVE-2026-43248, CVE-2026-43368, CVE-2026-43370, CVE-2026-46149, CVE-2026-52924, CVE-2026-53131, CVE-2026-53239, CVE-2026-53246, CVE-2026-53361, CVE-2026-63889, CVE-2026-63917, CVE-2026-63919, CVE-2026-63921, CVE-2026-64111, CVE-2026-68264, CVE-2026-68426, CVE-2026-74556, CVE-2026-63923, CVE-2026-64015, CVE-2026-68143, CVE-2026-68294, CVE-2026-72045)
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 systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:67723 https://access.redhat.com/errata/RHSA-2026:67604 https://access.redhat.com/errata/RHSA-2026:67603 https://access.redhat.com/errata/RHSA-2026:66376 https://access.redhat.com/errata/RHSA-2026:66357 https://access.redhat.com/errata/RHSA-2026:66375 https://access.redhat.com/errata/RHSA-2026:66356 https://access.redhat.com/errata/RHSA-2026:66350 https://access.redhat.com/errata/RHSA-2026:66351 https://access.redhat.com/errata/RHSA-2026:67471 https://access.redhat.com/errata/RHSA-2026:67470

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-86359, CVE-2026-71179, CVE-2026-71180, CVE-2026-71181, CVE-2026-71182, CVE-2026-86358, CVE-2026-81235, CVE-2026-81236, CVE-2026-81240, CVE-2026-81238, CVE-2026-81239, CVE-2026-81237)
Description	Dell 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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Repository Manager (DRM) versions prior to 3.5.2 Dell Update Package (DUP) Framework versions prior to 26.07.03 Dell Wyse Management Suite versions prior to WMS 2605.0.3.683 Dell Wyse Management Suite Repository versions prior to WMS 2605.0.3.119
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000509459/dsa-2026-419-security-update-for-dell-repository-manager-drm-vulnerability https://www.dell.com/support/kbdoc/en-us/000509455/dsa-2026-417-security-update-for-dell-update-package-dup-framework-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000502744/dsa-2026-387-security-update-for-dell-wyse-management-suite-wms-for-multiple-vulnerabilities

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-64423, CVE-2026-68138)
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 systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.4, 15.5 and 15.6 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP4 and 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP4, 15-SP5, 15-SP6 and 15-SP7 SUSE Linux Enterprise Micro 5.3, 5.4 and 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5, 15 SP6 and 15 SP7 SUSE Linux Enterprise Server 12 SP5, 15 SP4, 15 SP5, 15 SP6 and 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP4, 15 SP5, 15 SP6 and 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264193-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264192-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264185-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264183-1/

Vendor	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76676, CVE-2026-76677, CVE-2026-76678, CVE-2026-76679, CVE-2026-76680, CVE-2026-76681, CVE-2026-76682, CVE-2026-76683, CVE-2026-76684, CVE-2026-76685, CVE-2026-76686, CVE-2026-76687, CVE-2026-76688, CVE-2026-76689, CVE-2026-76690, CVE-2026-76691, CVE-2026-76692, CVE-2026-76693, CVE-2026-76694, CVE-2026-76695, CVE-2026-76696, CVE-2026-76697, CVE-2026-76698, CVE-2026-76699, CVE-2026-76700, CVE-2026-76701, CVE-2026-76702, CVE-2026-76703, CVE-2026-76704, CVE-2026-76705, CVE-2026-76706, CVE-2026-76707)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE Networking EdgeConnect SD-WAN Gateways • ECOS 9.7.x.x: 9.7.0.0 and below • ECOS 9.6.x.x: 9.6.3.1 and below • ECOS 9.5.x.x: 9.5.8.1 and below • ECOS 9.4.x.x: 9.4.8.2 and below HPE Networking EdgeConnect SD-WAN Orchestrator: • Orchestrator 9.7.x: 9.7.0 and below • Orchestrator 9.6.x: 9.6.3 and below • Orchestrator 9.5.x: 9.5.8 and below • Orchestrator 9.4.x: 9.4.10 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05135en_us&docLocale=en_US

Vendor	**Oracle**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle 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. Oracle advises to apply these security fixes at your earliest to protect your 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/cspusep2026.html

Vendor	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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 22.04 and 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8730-2 https://ubuntu.com/security/notices/USN-8761-1

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-10841, CVE-2026-11548, CVE-2026-11549, CVE-2026-11722, CVE-2026-15396, CVE-2026-15412, CVE-2026-15634, CVE-2026-11710, CVE-2026-11545, CVE-2026-16190, CVE-2026-15887, CVE-2026-16435, CVE-2026-16185, CVE-2026-9327, CVE-2026-9667, CVE-2026-9338, CVE-2026-16188, CVE-2026-9176, CVE-2026-11540, CVE-2026-11539, CVE-2026-11538, CVE-2026-11711, CVE-2026-16186, CVE-2026-16187, CVE-2026-11537, CVE-2026-16189, CVE-2026-9336, CVE-2026-66142, CVE-2026-66143, CVE-2026-66144, CVE-2026-65432, CVE-2026-43871, CVE-2026-48586, CVE-2026-14257, CVE-2026-69152, CVE-2026-66010, CVE-2026-44431, CVE-2026-44432, CVE-2026-41608, CVE-2026-66053)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak for Applications versions 1.0, 1.1, 5.1, 5.2, 5.3 Network Threat Analytics App for QRadar SIEM version 1.0.0 - 2.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7287579 https://www.ibm.com/support/pages/node/7287556 https://www.ibm.com/support/pages/node/7287565 https://www.ibm.com/support/pages/node/7287588 https://www.ibm.com/support/pages/node/7287605 https://www.ibm.com/support/pages/node/7287619 https://www.ibm.com/support/pages/node/7287494

Vendor	**NGINX**
Severity	**Medium**
Affected Vulnerability	NGINX ngx_http_v3_Module Vulnerability (CVE-2026-90439)
Description	NGINX has released a security update addressing a vulnerability that exists in their products. **CVE-2026-90439:** NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_v3_module module. When using HTTP/3 with OpenSSL versions <= OpenSSL 3.5.0 under certain configurations, a limited heap buffer overflow could happen while processing a TLS handshake. This can happen in a non-deterministic manner that is beyond the attacker's control. This may cause a heap buffer overflow in the NGINX worker process leading to a restart and/or limited data corruption. NGINX advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NGINX Open Source 1.30.4 and 1.29.2 to 1.31.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000162604

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.