Advisory Alert

Alert Number: AAA20260902 **Date:** September 2, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
SonicWall	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Improper Input Validation Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
HPE	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76657, CVE-2026-76658, CVE-2026-19766, CVE-2026-73700, CVE-2026-73701, CVE-2026-73749)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• HPE Networking Fabric Composer 7.3.3 and prior • HPE Networking AOS-CX: 10.18.0001, 10.17.1021 & below, 10.16.1051 & below, 10.13.1180 & below, 10.10.1180 & below (EOM)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05133en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05134en_us&docLocale=en_US

Vendor	**SonicWall**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-83548, CVE-2026-83549)
Description	SonicWall has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-83548:** A Pre-authentication SSRF vulnerability exists in the SMA1000 Appliance Work Place interface due to an unintended alternate access path. A remote unauthenticated attacker could potentially exploit this vulnerability to gain unauthorized access to sensitive functionality and perform unauthorized operations.. **CVE-2026-83549:** Post-authentication Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) which in specific conditions could potentially enable a remote authenticated attacker as administrator to execute arbitrary OS commands, resulting in remote code execution. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SonicWall SMA1000 Models (6210, 7210, 8200v): 12.4.3-03453 (platform-hotfix) & earlier 12.5.0-02835 (platform-hotfix) & earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Improper Input Validation vulnerability (CVE-2025-66614)
Description	IBM has released a security update addressing a vulnerability that exist in their products. **CVE-2025-66614:** If Tomcat was configured with more than one virtual host and the TLS configuration for one of those hosts did not require client certificate authentication but another one did, it was possible for a client to bypass the client certificate authentication by sending different host names in the SNI extension and the HTTP host header field. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QRadar versions 7.5.0 - 7.5.0 UP15 IF06
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7286010

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-74480, CVE-2026-64002, CVE-2026-15809, CVE-2026-34986, CVE-2025-21834, CVE-2026-23003, CVE-2026-43450, CVE-2026-43454, CVE-2026-45970, CVE-2026-46120, CVE-2026-53026, CVE-2026-53053, CVE-2026-53153, CVE-2026-53185, CVE-2026-53189, CVE-2026-53196, CVE-2026-53391, CVE-2026-53392, CVE-2026-53397, CVE-2026-53399, CVE-2026-63800, CVE-2026-64018, CVE-2026-64136, CVE-2026-64189, CVE-2026-64276, CVE-2026-64277, CVE-2026-64298, CVE-2026-64304, CVE-2026-64320, CVE-2026-64384, CVE-2026-64418, CVE-2026-64438, CVE-2026-64490, CVE-2026-68086, CVE-2026-68166, CVE-2026-68480, CVE-2026-72069, CVE-2026-72130)
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	• Red Hat Enterprise Linux 8.4 (Advanced Update Support, Extended Life Cycle Long Life): x86_64 • Red Hat Enterprise Linux 8.6 (Advanced Update Support, Extended Life Cycle Long Life): x86_64 • Red Hat Enterprise Linux 8.8 (Extended Life Cycle Long Life, Telco Update Support, Update Services for SAP Solutions): x86_64, ppc64le • Red Hat Enterprise Linux 9.4 (Advanced Update Support, Update Services for SAP Solutions, Four Years of Updates, Extended Life Cycle): x86_64, aarch64, ppc64le, s390x • Red Hat Enterprise Linux 10 Base & CodeReady Builder: x86_64, aarch64, ppc64le, s390x • Red Hat Enterprise Linux 10.2 (Extended Update Support, Four Years of Support/Updates, Extended Life Cycle, and CodeReady Linux Builder Extended Update Support): x86_64, aarch64, ppc64le, s390x • Red Hat OpenShift Container Platform 4.20 (RHEL 8 / RHEL 9): x86_64, aarch64, ppc64le, s390x • Red Hat OpenShift Container Platform 4.21 (RHEL 9): x86_64, aarch64, ppc64le, s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:62372 https://access.redhat.com/errata/RHSA-2026:62346 https://access.redhat.com/errata/RHSA-2026:62345 https://access.redhat.com/errata/RHSA-2026:60449 https://access.redhat.com/errata/RHSA-2026:60444 https://access.redhat.com/errata/RHSA-2026:61973 https://access.redhat.com/errata/RHSA-2026:61959 https://access.redhat.com/errata/RHSA-2026:61887

Vendor	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-73753, CVE-2026-73752, CVE-2026-73751, CVE-2026-73782, CVE-2026-73750, CVE-2026-73781, CVE-2026-73780, CVE-2026-73779, CVE-2026-73778, CVE-2026-73777, CVE-2026-73776, CVE-2026-73775, CVE-2026-73774, CVE-2026-73773, CVE-2026-73771, CVE-2026-73770, CVE-2026-73768, CVE-2026-73767, CVE-2026-73766, CVE-2026-73765, CVE-2026-73763, CVE-2026-73764, CVE-2026-73762, CVE-2026-73760, CVE-2026-73758, CVE-2026-73759, CVE-2026-73761, CVE-2026-73772, CVE-2026-73757, CVE-2026-73756, CVE-2026-73755, CVE-2026-73754, CVE-2026-73783, CVE-2026-73704, CVE-2026-73702, CVE-2026-73703, CVE-2026-73705, CVE-2026-73706, CVE-2026-73707, CVE-2026-73708, CVE-2026-73709, CVE-2026-73710, CVE-2026-73712, CVE-2026-73711, CVE-2026-73713, CVE-2026-73714, CVE-2026-73717, CVE-2026-73716, CVE-2026-73715, CVE-2026-73718, CVE-2026-73721, CVE-2026-73720, CVE-2026-73719, CVE-2026-73722, CVE-2026-73724, CVE-2026-73723, CVE-2026-73725, CVE-2026-73726, CVE-2026-73730, CVE-2026-73729, CVE-2026-73728, CVE-2026-73731, CVE-2026-73732, CVE-2026-73734, CVE-2026-73733, CVE-2026-73735, CVE-2026-73736, CVE-2026-73737, CVE-2026-73738, CVE-2026-73740, CVE-2026-73739, CVE-2026-73742, CVE-2026-73741, CVE-2026-73743, CVE-2026-73744, CVE-2026-73745, CVE-2026-73746, CVE-2026-73747, CVE-2026-73748)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• HPE Networking Fabric Composer 7.3.3 and prior • HPE Networking AOS-CX: 10.18.0001, 10.17.1021 & below, 10.16.1051 & below, 10.13.1180 & below, 10.10.1180 & below (EOM)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05133en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05134en_us&docLocale=en_US

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-34477, CVE-2026-34478, CVE-2026-34480, CVE-2026-5588, CVE-2025-9714, CVE-2026-24733, CVE-2026-24734, CVE-2026-34282, CVE-2026-22016, CVE-2026-23865, CVE-2026-22021, CVE-2026-22013, CVE-2026-22018, CVE-2026-22008, CVE-2026-34268, CVE-2026-22007, CVE-2026-6918, CVE-2025-61984, CVE-2025-61985, CVE-2026-34479, CVE-2025-33141, CVE-2026-18567, CVE-2026-16660, CVE-2026-17483)
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	QRadar versions 7.5.0 - 7.5.0 UP15 IF06 IBM Db2 Mirror for i versions 7.4, 7.5, and 7.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7286010 https://www.ibm.com/support/pages/node/7286014 https://www.ibm.com/support/pages/node/7285904

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.