Advisory Alert

Alert Number: AAA20250901 **Date:** September 1, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
NetApp	**High**, Medium	Multiple Vulnerabilities
QNAP	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
F5	Medium	Denial of Service Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-29927, CVE-2024-51504, CVE-2025-7783)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in the User Entity Behavior Analytics app for IBM QRadar SIEM. **CVE-2025-29927** - Next.js is a React framework for building full-stack web applications. Starting in version 1.11.4 and prior to versions 12.3.5, 13.5.9, 14.2.25, and 15.2.3, it is possible to bypass authorization checks within a Next.js application, if the authorization check occurs in middleware. If patching to a safe version is infeasible, it is recommend that you prevent external user requests which contain the x-middleware-subrequest header from reaching your Next.js application. **CVE-2024-51504** - When using IPAuthenticationProvider in ZooKeeper Admin Server there is a possibility of Authentication Bypass by Spoofing -- this only impacts IP based authentication implemented in ZooKeeper Admin Server. Default configuration of client's IP address detection in IPAuthenticationProvider, which uses HTTP request headers, is weak and allows an attacker to bypass authentication via spoofing client's IP address in request headers. Default configuration honors X-Forwarded-For HTTP header to read client's IP address. X-Forwarded-For request header is mainly used by proxy servers to identify the client and can be easily spoofed by an attacker pretending that the request comes from a different IP address. Admin Server commands, such as snapshot and restore arbitrarily can be executed on successful exploitation which could potentially lead to information leakage or service availability issues. **CVE-2025-7783** - Use of Insufficiently Random Values vulnerability in form-data allows HTTP Parameter Pollution (HPP). This vulnerability is associated with program files lib/form_data.Js. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	User Entity Behavior Analytics app versions 1.0.0 - 4.1.17 for IBM QRadar SIEM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7243582

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
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 system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Real Time Module 15-SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-202503023-1/

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-26466, CVE-2025-32415, CVE-2024-55549)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-26466** - Multiple NetApp products incorporate OpenSSH. OpenSSH versions 9.5p1 through 9.9p1 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). **CVE-2025-32415** - Multiple NetApp products incorporate libxml2. Libxml2 versions prior to 2.13.8 and 2.14.0 prior to 2.14.2 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). **CVE-2024-55549** - Multiple NetApp products incorporate libxslt. Libxslt versions prior to 1.1.43 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9 NetApp Manageability SDK
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250228-0002 • https://security.netapp.com/advisory/ntap-20250605-0003 • https://security.netapp.com/advisory/ntap-20250613-0007

Affected Product	**QNAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-29893, CVE-2025-29894, CVE-2025-29898, CVE-2025-30260, CVE-2025-30275, CVE-2025-30277, CVE-2025-30278, CVE-2025-33033, CVE-2025-33036, CVE-2025-33037, CVE-2025-33038, CVE-2025-30261, CVE-2025-30262, CVE-2025-30263, CVE-2025-29874, CVE-2025-29875, CVE-2025-29878, CVE-2025-29879, CVE-2025-29886, CVE-2025-29888, CVE-2025-29889, CVE-2025-29890, CVE-2025-29899, CVE-2025-29900, CVE-2025-29882, CVE-2025-30264, CVE-2025-30265, CVE-2025-30267, CVE-2025-30268, CVE-2025-30270, CVE-2025-30271, CVE-2025-30272, CVE-2025-30273, CVE-2025-30274, CVE-2025-33032, CVE-2025-29901, CVE-2025-47206)
Description	QNAP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause SQL Injection, Denial of Service, Information Disclosure, arbitrary commands execution, memory corruption. QNAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Qsync Central 4.5.x File Station 5 version 5.5.x QTS 5.2.x QuTS hero h5.2.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.qnap.com/en/security-advisory/qsa-25-22 • https://www.qnap.com/en/security-advisory/qsa-25-28 • https://www.qnap.com/en/security-advisory/qsa-25-19 • https://www.qnap.com/en/security-advisory/qsa-25-21 • https://www.qnap.com/en/security-advisory/qsa-25-31

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-48949, CVE-2025-48050, CVE-2024-55565, CVE-2024-43799, CVE-2024-36114, CVE-2022-1471, CVE-2023-43642, CVE-2024-9823, CVE-2024-6762, CVE-2017-18214, CVE-2022-24785, CVE-2022-31129, CVE-2023-22467, CVE-2024-45813, CVE-2025-27152, CVE-2023-26133, CVE-2019-9193, CVE-2023-32305, CVE-2021-3393, CVE-2022-2625, CVE-2025-50181, CVE-2025-50182, CVE-2025-48068, CVE-2024-51479, CVE-2022-24823, CVE-2022-41881, CVE-2023-34462)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in the User Entity Behavior Analytics app for IBM QRadar SIEM. These vulnerabilities could be exploited by malicious users to cause authorization bypass, code execution, Denial of Service, Information Disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	User Entity Behavior Analytics app versions 1.0.0 - 4.1.17 for IBM QRadar SIEM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7243582

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2025-54500)
Description	F5 has released security updates addressing a Denial of Service vulnerability that exists in HTTP/2 which affects F5 products. **CVE-2025-54500** - An HTTP/2 implementation flaw allows a denial-of-service (DoS) that uses malformed HTTP/2 control frames to break the maximum concurrent streams limit (HTTP/2 MadeYouReset Attack). F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next (all modules) 20.3.0 BIG-IP Next SPK versions 2.0.0 - 2.0.2 and 1.7.0 - 1.9.2 BIG-IP Next CNF versions 2.0.0 - 2.0.2 and 1.1.0 - 1.4.1 BIG-IP Next for Kubernetes 2.0.0 BIG-IP (all modules) versions 17.5.0 - 17.5.1, 17.1.0 - 17.1.2 and 16.1.0 - 16.1.6 F5 Silverline (all services)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000152001

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.