Advisory Alert

Alert Number: AAA20260922 **Date:** September 22, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities
F5	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-75899, CVE-2026-75931, CVE-2026-75975, CVE-2026-76172, CVE-2026-73646, CVE-2026-67213, CVE-2026-67214, CVE-2026-69153, CVE-2026-75838)
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 Verify Identity Access Digital Credentials - Versions 24.06 - 26.07 IBM Security QRadar Log Management AQL Plugin - Versions 1.0.0 - 1.1.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7288771 • https://www.ibm.com/support/pages/node/7288723

Vendor	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-3833, CVE-2026-33845)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-3833:** A flaw was found in gnutls. This vulnerability occurs because gnutls performs case-sensitive comparisons of `nameConstraints` labels, specifically for `dNSName` (DNS) or `rfc822Name` (email) constraints within `excludedSubtrees` or `permittedSubtrees`. A remote attacker can exploit this by crafting a leaf certificate with casing differences in the Subject Alternative Name (SAN), leading to a policy bypass where a certificate that should be rejected is instead accepted. This could result in unauthorized access or information disclosure. **CVE-2026-33845:** A flaw in GnuTLS DTLS handshake parsing allows malformed fragments with zero length and non-zero offset, leading to an integer underflow during reassembly and resulting in an out-of-bounds read. This issue is remotely exploitable and may cause information disclosure or denial of service. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS - Version 2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000163346 • https://my.f5.com/manage/s/article/K000163347

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, 24.04, 26.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8793-1 • https://ubuntu.com/security/notices/USN-8761-3 • https://ubuntu.com/security/notices/USN-8730-4 • https://ubuntu.com/security/notices/USN-8726-3 • https://ubuntu.com/security/notices/USN-8729-3

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.