Security Bulletin: Multiple vulnerabilities have been addressed in IBM Aspera Shares

Security Bulletin

Summary

Multiple vulnerabilities have been addressed in IBM Aspera Shares Version 1.11.1

Vulnerability Details

CVEID: CVE-2025-13916 *(https://www.cve.org/CVERecord?id=CVE-2025-13916)*

DESCRIPTION: IBM Aspera Shares uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2026-25500 *(https://www.cve.org/CVERecord?id=CVE-2026-25500)*

DESCRIPTION: Rack is a modular Ruby web server interface. Prior to versions 2.2.22, 3.1.20, and 3.2.5, `Rack::Directory` generates an HTML directory index where each file entry is rendered as a clickable link. If a file exists on disk whose basename starts with the `javascript:` scheme (e.g. `javascript:alert(1)`), the generated index contains an anchor whose `href` is exactly `javascript:alert(1)`. Clicking the entry executes JavaScript in the browser (demonstrated with `alert(1)`). Versions 2.2.22, 3.1.20, and 3.2.5 fix the issue.

CWE: CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(https://cwe.mitre.org/data/definitions/79.html)*

CVSS Source: security-advisories@github.com

CVSS Base score: 5.4

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2025-61594 *(https://www.cve.org/CVERecord?id=CVE-2025-61594)*

CVEID: CVE-2025-66487 *(https://www.cve.org/CVERecord?id=CVE-2025-66487)*

DESCRIPTION: IBM Aspera Shares does not properly rate limit the frequency that an authenticated user can send emails, which could result in email flooding or a denial of service.

CWE: CWE-770: Allocation of Resources Without Limits or Throttling *(https://cwe.mitre.org/data/definitions/770.html)*

CVSS Source: IBM

CVSS Base score: 2.7

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2025-66485 *(https://www.cve.org/CVERecord?id=CVE-2025-66485)*

DESCRIPTION: IBM Aspera Shares is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.

CWE: CWE-644: Improper Neutralization of HTTP Headers for Scripting Syntax *(https://cwe.mitre.org/data/definitions/644.html)*

Get Notified about Future Security Bulletins

Subscribe to My Notifications *(https://www.ibm.com/support/pages/node/718119)* to be notified of important product support alerts like this.

References

Complete CVSS v3 Guide

On-line Calculator v3

Related Information

IBM Secure Engineering Web Portal *(http://www.ibm.com/security/secure-engineering/bulletins.html)*

IBM Product Security Incident Response Blog *(http://www.ibm.com/blogs/psirt)*

Acknowledgement

Change History

27 Mar 2026: Initial Publication

Cross-reference information

Product	Component	Platform	Version
IBM Aspera		Linux	1.0
IBM Aspera Enterprise		Linux	1.0.2
IBM Aspera Enterprise On Demand		Linux	1.1
IBM Aspera Shares		Linux; Windows	1.11.1
IBM Aspera on Demand		Linux	1.0