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
CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(https://cwe.mitre.org/data/definitions/327.html)*
CVSS Source: IBM
CVSS Base score: 5.9
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2025-66486 *(https://www.cve.org/CVERecord?id=CVE-2025-66486)*
DESCRIPTION: IBM Aspera Shares is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site.
CWE: CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) *(https://cwe.mitre.org/data/definitions/80.html)*
CVSS Source: IBM
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2026-22860 *(https://www.cve.org/CVERecord?id=CVE-2026-22860)*
DESCRIPTION: Rack is a modular Ruby web server interface. Prior to versions 2.2.22, 3.1.20, and 3.2.5, `Rack::Directory`'s path check used a string prefix match on the expanded path. A request like `/../root_example/` can escape the configured root if the target path starts with the root string, allowing directory listing outside the intended root. Versions 2.2.22, 3.1.20, and 3.2.5 fix the issue.
CWE: CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(https://cwe.mitre.org/data/definitions/22.html)*
CVSS Source: security-advisories@github.com
CVSS Base score: 7.5

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)*

DESCRIPTION: URI is a module providing classes to handle Uniform Resource Identifiers. In versions prior to 0.12.5, 0.13.3, and 1.0.4, a bypass exists for the fix to CVE-2025-27221 that can expose user credentials. When using the `+` operator to combine URIs, sensitive information like passwords from the original URI can be leaked, violating RFC3986 and making applications vulnerable to credential exposure. Versions 0.12.5, 0.13.3, and 1.0.4 fix the issue.

CWE: CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(https://cwe.mitre.org/data/definitions/212.html)*

CVSS Source: NVD

CVSS Base score: 7.5

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

CVEID: CVE-2025-66483 *(https://www.cve.org/CVERecord?id=CVE-2025-66483)*

DESCRIPTION: IBM Aspera Shares does not invalidate session after a password reset which could allow an authenticated user to impersonate another user on the system.

CWE: CWE-613: Insufficient Session Expiration *(https://cwe.mitre.org/data/definitions/613.html)*

CVSS Source: IBM

CVSS Base score: 6.3

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

CVEID: CVE-2025-66484 *(https://www.cve.org/CVERecord?id=CVE-2025-66484)*

DESCRIPTION: IBM Aspera Shares is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.

CVSS Source: IBM

CVSS Base score: 5.5

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

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)*

CVSS Source: IBM

CVSS Base score: 5.4

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

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Aspera Shares	1.9.9 - 1.11.0

Remediation/Fixes

Product(s)	Fixing VRM	Platform	Link to Fix
IBM Aspera Shares	1.11.1	Windows	click here *(https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=ibm%7EOther%20software&product=ibm/Other+software/Aspera+Shares&release=1.11.1&platform=Windows&function=all)*
IBM Aspera Shares	1.11.1	Linux	click here *(https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=ibm%7EOther%20software&product=ibm/Other+software/Aspera+Shares&release=1.11.1&platform=Linux&function=all)*

Workarounds and Mitigations

None

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

*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

Disclaimer

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES ""AS IS"" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. In addition to other efforts to address potential vulnerabilities, IBM periodically updates the record of components contained in our product offerings. As part of that effort, if IBM identifies previously unidentified packages in a product/service inventory, we address relevant vulnerabilities regardless of CVE date. Inclusion of an older CVEID does not demonstrate that the referenced product has been used by IBM since that date, nor that IBM was aware of a vulnerability as of that date. We are making clients aware of relevant vulnerabilities as we become aware of them. "Affected Products and Versions" referenced in IBM Security Bulletins are intended to be only products and versions that are supported by IBM and have not passed their end-of-support or warranty date. Thus, failure to reference unsupported or extended-support products and versions in this Security Bulletin does not constitute a determination by IBM that they are unaffected by the vulnerability. Reference to one or more unsupported versions in this Security Bulletin shall not create an obligation for IBM to provide fixes for any unsupported or extended-support products or versions.

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

Document Information

More support for:

IBM Aspera Shares *(https://www.ibm.com/mysupport/s/topic/0TO50000000IYjLGAW)*

Software version:

1.11.1

Operating system(s):

Linux, Windows

Document number:

7267848

Modified date:

27 March 2026

Initial Publish date:

27 March 2026