



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) (<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

About cookies on this site

Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising. For more information, please review your [cookie preferences](#) options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](https://www.ibm.com/us-en/privacy/ccp) (<https://www.ibm.com/us-en/privacy/ccp>)

In addition to the services they provide to IBM, certain IBM authorized partners may also use these cookies for their own purposes. This activity may qualify as a "sale" or "sharing" under the California Consumer Privacy Act "CCPA". By selecting "Do not sell or share my personal information", you are requesting IBM to use required cookies only.

To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed [here](#).

Accept all

Do not sell or share my personal 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) (<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) (<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) (<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 URI module, sensitive information like passwords from the original URI can be vulnerable to credential exposure. Versions 0.12.5, 0.13.3, and 1.0.4 fix the issue.



About cookies on this site

Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising. For more information, please review your options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](https://www.ibm.com/us-en/privacy/ccpa) (<https://www.ibm.com/us-en/privacy/ccpa>)

In addition to the services they provide to IBM, certain IBM authorized partners may also use these cookies for their own purposes. This activity may qualify as a "sale" or "sharing" under the California Consumer Privacy Act "CCPA". By selecting "Do not sell or share my personal information", you are requesting IBM to use required cookies only.

To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed [here](#).

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 credential exposure 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) (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) (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) (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)

(https://cwe.mitre.org/data/definitions/644.html)

CVSS Source: IBM

CVSS Base score: 5.4

About cookies on this site
Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising. For more information, please review your options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](https://www.ibm.com/us-en/privacy/ccpa) (https://www.ibm.com/us-en/privacy/ccpa)

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

In addition to the services they provide to IBM, certain IBM authorized partners may also use these cookies for their own purposes. This activity may qualify as a "sale" or "sharing" under the California Consumer Privacy Act "CCPA". By selecting "Do not sell or share my personal information", you are requesting IBM to use required cookies only.

Fixing VRM 1.11.1

Platform Windows

Link to Fix [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)

(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)

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)

(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)

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**About cookies on this site**

Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising. For more information, please review your

In addition to the services they provide to IBM, certain IBM authorized partners may also use these cookies for their own purposes.

This activity may qualify as a "sale" or "sharing" under the California Consumer Privacy Act "CCPA". By selecting "Do not sell or share my personal information", you are requesting IBM to use required cookies only.

To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed [here](#).

options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](#)

(<https://www.ibm.com/us-en/privacy/ccpa>)