Security Bulletin: Security Vulnerabilities have been found in IBM Verify Identity Access and IBM Security Verify Access

Security Bulletin

Summary

Security Vulnerabilities have been addressed in IBM Verify Identity Access and IBM Security Verify Access

Vulnerability Details

CVEID: CVE-2025-12635 *(https://www.cve.org/CVERecord?id=CVE-2025-12635)*

DESCRIPTION: IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 25.0.0.12 are affected by cross-site scripting due to improper validation of user-supplied input. An attacker could exploit this vulnerability by using a specially crafted URL to redirect the user to a malicious site.

a patch for this issue. As a workaround, configure crypto-js to use SHA256 with at least 250,000 iterations.

CWE: CWE-328: Use of Weak Hash *(https://cwe.mitre.org/data/definitions/328.html)*

CVSS Source: IBM X-Force

CVSS Base score: 9.1

CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVEID: CVE-2026-2475 *(https://www.cve.org/CVERecord?id=CVE-2026-2475)*

DESCRIPTION: IBM Verify Identity Access could allow a remote attacker to conduct phishing attacks, caused by an open redirect vulnerability. An attacker could exploit this vulnerability using a specially crafted request to redirect a victim to arbitrary Web sites.

CWE: CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(https://cwe.mitre.org/data/definitions/601.html)*

CVSS Source: IBM

CVSS Base score: 3.1

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

update, insert, delete, or read operations on accessible data, caused by an easily exploitable vulnerability.

CVSS Source: secalert_us@oracle.com

CVSS Base score: 6.1

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

CVEID: CVE-2026-21925 *(https://www.cve.org/CVERecord?id=CVE-2026-21925)*

DESCRIPTION: Java SE could allow a remote unauthenticated attacker to bypass security controls and perform unauthorized update, insert, delete, or read operations on accessible data, caused by an difficult to exploit vulnerability.

CVSS Source: secalert_us@oracle.com

CVSS Base score: 4.8

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

CVEID: CVE-2026-1343 *(https://www.cve.org/CVERecord?id=CVE-2026-1343)*

DESCRIPTION: IBM Security Verify access allows an attacker to contact internal authentication endpoints which are protected by the Reverse Proxy.

CVEID: CVE-2026-1346 *(https://www.cve.org/CVERecord?id=CVE-2026-1346)*

DESCRIPTION: IBM Security Verify Access Container could allow a locally authenticated user to escalate their privileges to root due to execution with unnecessary privileges than required.

CWE: CWE-250: Execution with Unnecessary Privileges *(https://cwe.mitre.org/data/definitions/250.html)*

CVSS Source: IBM

CVSS Base score: 9.3

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

CVEID: CVE-2026-1345 *(https://www.cve.org/CVERecord?id=CVE-2026-1345)*

DESCRIPTION: IBM Security Verify Access Container could allow an unauthenticated user to execute arbitrary commands as lower user privileges on the system due to improper validation of user supplied input.

CWE: CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(https://cwe.mitre.org/data/definitions/78.html)*

CVSS Source: IBM

CVSS Base score: 7.3

IBM Security Verify Access	10.0 - 10.0.9.1

Remediation/Fixes

IBM encourages customers to update their systems promptly.

Appliance:

Affected Products and Versions	Fix availability
IBM Verify Identity Access 11.0 - 11.0.2	Download IBM Verify Identity Access v11.0.2 IF1 *(https://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FTivoli%2FIBM+Verify+Identity+Access&fixids=11.0.2.0-ISS-IVIA-IF0001&source=SAR)*
IBM Security Verify Access 10.0 - 10.0.9.1	Download IBM Security Verify Access v10.0.9.1 IF1 *(https://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FTivoli%2FIBM+Security+Verify+Access&fixids=10.0.9.1-ISS-ISVA-IF0001&source=SAR)*

Change History

31 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 for that date or that IBM was aware of a vulnerability as of that date. We are making IBM aware of Security Vulnerabilities we become aware of them. "Affected Products and Versions" refer to the IBM Security Bulletins are intended to be only products and versions that are supported by IBM and which have not passed their support or service date. Thus, failure to reference unsupported or extended-support products and versions in a Security Bulletin does not constitute a determination by IBM that they are unaffected by the vulnerabilities identified in the Bulletin. Reference to unsupported versions in this Security Bulletin shall not create any obligation for IBM to provide fixes for any unsupported or extended-support products or versions.

Document number:

7268253

Modified date:

31 March 2026

Initial Publish date:

31 March 2026