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.
CWE: CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(https://cwe.mitre.org/data/definitions/79.html)*
CVSS Source: IBM
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-2026-2862 *(https://www.cve.org/CVERecord?id=CVE-2026-2862)*
DESCRIPTION: IBM Security Verify could allow a remote attacker to access sensitive information due to an inconsistent interpretation of an HTTP request by a reverse proxy.
CWE: CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') *(https://cwe.mitre.org/data/definitions/444.html)*
CVSS Source: IBM
CVSS Base score: 5.3
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVEID: CVE-2023-46233 *(https://www.cve.org/CVERecord?id=CVE-2023-46233)*
DESCRIPTION: crypto-js is a JavaScript library of crypto standards. Prior to version 4.2.0, crypto-js PBKDF2 is 1,000 times weaker than originally specified in 1993, and at least 1,300,000 times weaker than current industry standard. This is because it both defaults to SHA1, a cryptographic hash algorithm considered insecure since at least 2005, and defaults to one single iteration, a 'strength' or 'difficulty' value specified at 1,000 when specified in 1993. PBKDF2 relies on iteration count as a countermeasure to preimage and collision attacks. If used to protect passwords, the impact is high. If used to generate signatures, the impact is high. Version 4.2.0 contains

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)

CVEID: CVE-2026-1342 *(https://www.cve.org/CVERecord?id=CVE-2026-1342)*

DESCRIPTION: IBM Security Verify Access Container could allow a locally authenticated user to execute malicious scripts from outside of its control sphere.

CWE: CWE-829: Inclusion of Functionality from Untrusted Control Sphere *(https://cwe.mitre.org/data/definitions/829.html)*

CVSS Source: IBM

CVSS Base score: 8.5

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

CVEID: CVE-2026-21945 *(https://www.cve.org/CVERecord?id=CVE-2026-21945)*

DESCRIPTION: Java SE is vulnerable to a denial of service, caused by an easily exploitable vulnerability issue that allows an remote attacker to cause a hang or repeatable crash of the application.

CWE: CWE-400: Uncontrolled Resource Consumption *(https://cwe.mitre.org/data/definitions/400.html)*

CVSS Source: secalert_us@oracle.com

CVSS Base score: 7.5

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

CVEID: CVE-2026-21932 *(https://www.cve.org/CVERecord?id=CVE-2026-21932)*

DESCRIPTION: Java SE could allow a remote attacker to bypass security controls and create, delete, or modify critical data or all accessible data, caused by an easily exploitable vulnerability.

CVSS Source: secalert_us@oracle.com

CVSS Base score: 7.4

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

CVEID: CVE-2026-21933 *(https://www.cve.org/CVERecord?id=CVE-2026-21933)*

DESCRIPTION: Java SE could allow a remote attacker to bypass security controls and perform unauthorized

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.
CWE: CWE-918: Server-Side Request Forgery (SSRF) *(https://cwe.mitre.org/data/definitions/918.html)*
CVSS Source: IBM
CVSS Base score: 7.2
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N)

CVEID: CVE-2026-1491 *(https://www.cve.org/CVERecord?id=CVE-2026-1491)*
DESCRIPTION: IBM Security Verify could allow a remote attacker to access sensitive information due to an inconsistent interpretation of an HTTP request by a reverse proxy.
CWE: CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') *(https://cwe.mitre.org/data/definitions/444.html)*
CVSS Source: IBM
CVSS Base score: 5.3
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVEID: CVE-2026-1188 *(https://www.cve.org/CVERecord?id=CVE-2026-1188)*
DESCRIPTION: In the Eclipse OMR port library component since release 0.2.0, an API function to return the textual names of all supported processor features was not accounting for the separator inserted between processor features. If the output buffer supplied to this function was incorrectly sized, failing to account for the separator when determining when a write to the buffer was safe could lead to a buffer overflow. This issue is fixed in Eclipse OMR version 0.8.0.
CWE: CWE-131: Incorrect Calculation of Buffer Size *(https://cwe.mitre.org/data/definitions/131.html)*
CVSS Source: NVD
CVSS Base score: 9.8
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

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

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

CVEID: CVE-2026-4101 *(https://www.cve.org/CVERecord?id=CVE-2026-4101)*

DESCRIPTION: IBM Security Verify Access under certain load conditions could allow an attacker to bypass authentication mechanisms and gain unauthorized access to the application.

CWE: CWE-287: Improper Authentication *(https://cwe.mitre.org/data/definitions/287.html)*

CVSS Source: IBM

CVSS Base score: 8.1

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

CVEID: CVE-2026-4364 *(https://www.cve.org/CVERecord?id=CVE-2026-4364)*

DESCRIPTION: IBM Security Verify Access allows certificate listings retrieved via a browser session to return a JSON payload while incorrectly specifying the response Content-Type as text/html. Because the content is delivered with an HTML MIME type, browsers may interpret the JSON data as executable script under certain conditions. This creates an opportunity for JavaScript injection, potentially leading to cross-site scripting (XSS).

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

CVSS Source: IBM

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)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Verify Identity Access Container	11.0 - 11.0.2
IBM Security Verify Access Container	10.0 - 10.0.9.1
IBM Verify Identity Access	11.0 - 11.0.2

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)*

Container:

Container Download *(https://docs.verify.ibm.com/ibm-security-verify-access/docs/containers)*

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

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 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 Security Verify Access		Platform Independent	10.0.9.1 IF1
IBM Verify Identity Access		Platform Independent	11.0.2 IF1

Document Information

More support for:

IBM Verify Identity Access *(https://www.ibm.com/mysupport/s/topic/0TO500000002601GAA)*

Software version:

11.0.2 IF1

Document number:

7268253

Modified date:

31 March 2026

Initial Publish date:

31 March 2026