Security Bulletin: Security vulnerability has been detected in IBM Security Verify Directory (Container) (CVE-2025-36074)

Security Bulletin

Summary

Security vulnerability has been addressed in IBM Security Verify Directory (Container)

Vulnerability Details

CVEID: CVE-2025-36074 *(https://www.cve.org/CVERecord?id=CVE-2025-36074)*

DESCRIPTION: IBM Security Verify Directory could be vulnerable to malicious file upload by not validating file type. A privileged user could upload malicious files into the system that can be sent to victims for performing further attacks against the system.

CWE: CWE-434: Unrestricted Upload of File with Dangerous Type *(https://cwe.mitre.org/data/definitions/434.html)*

CVSS Source: IBM

CVSS Base score: 5.5

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

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Security Verify Directory (Container)	10.0.0 - 10.0.0.3

Remediation/Fixes

IBM strongly encourages customers to update their systems promptly.

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

08 Apr 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 customers 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 reached their end-of-support or warranty date. Vulnerability scanning may lead 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 vulnerabilities identified. IBM may support one or more fixes in this Security Bulletin shall not create an obligation for IBM to provide fixes for any unsupported or extended-support products or versions.

Document Information

More support for:

IBM Security Verify Directory *(https://www.ibm.com/mysupport/s/topic/0TO5000000025yAGAQ)*

Software version:

10.0.4

Document number:

7268907

Modified date:

08 April 2026

Initial Publish date:

08 April 2026