Security Bulletin: Multiple Vulnerabilities in IBM Guardium Key Lifecycle Manager (CVE-2025-68161, CVE-2026-1726)

Created by PSIRT Functional ID on Tue, 04/07/2026 - 02:29
Published URL: https://www.ibm.com/support/pages/node/7268697

Security Bulletin

Summary

Security Vulnerabilities have been addressed in IBM Guardium Key Lifecycle Manager

Vulnerability Details

CVEID: CVE-2025-68161 *(https://www.cve.org/CVERecord?id=CVE-2025-68161)*

DESCRIPTION: The Socket Appender in Apache Log4j Core versions 2.0-beta9 through 2.25.2 does not perform TLS hostname verification of the peer certificate, even when the verifyHostName https://logging.apache.org/log4j/2.x/manual/appenders/network.html#SslConfiguration-attr-verifyHostName configuration attribute or the log4j2.sslVerifyHostName https://logging.apache.org/log4j/2.x/manual/systemproperties.html#log4j2.sslVerifyHostName system property is set to true. This issue may allow a man-in-the-middle attacker to intercept or redirect log traffic under the following conditions: * The attacker is able to intercept or redirect network traffic between the client and the log receiver. * The attacker can present a server certificate issued by a certification authority trusted by the Socket Appender's configured trust store (or by the default Java trust store if no custom trust store is configured). Users are advised to upgrade to Apache Log4j Core version 2.25.3, which addresses this issue. As an alternative mitigation, the Socket Appender may be configured to use a private or restricted trust root to limit the set of trusted certificates.

CWE: CWE-297: Improper Validation of Certificate with Host Mismatch *(https://cwe.mitre.org/data/definitions/297.html)*

CVSS Source: NVD

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-2026-1726 *(https://www.cve.org/CVERecord?id=CVE-2026-1726)*

DESCRIPTION:

CWE: CWE-269: Improper Privilege Management *(https://cwe.mitre.org/data/definitions/269.html)*

CVSS Source: IBM

CVSS Base score: 6.4

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

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Guardium Key Lifecycle Manager	4.1
IBM Guardium Key Lifecycle Manager	4.1.1
IBM Guardium Key Lifecycle Manager	4.2
IBM Guardium Key Lifecycle Manager	4.2.1
IBM Guardium Key Lifecycle Manager	5.0
IBM Guardium Key Lifecycle Manager	5.1

Remediation/Fixes

IBM encourages customers to update their systems promptly.

<table>
<tr><th>Principal Product and Version(s)</th><th>Remediation/Fixes</th></tr>
<tr><td>IBM Guardium Key Lifecycle Manager (GKLM) v4.1</td><td rowspan="4">1. Download IBM Guardium Key Lifecycle Manager (GKLM) v5.1
(https://www.ibm.com/software/passportadvantage/pao-customer)
(the product is available for download through IBM Passport Advantage)
(https://www.ibm.com/software/passportadvantage/pao-customer)

2. Apply 5.1.0-ISS-GKLM-FP0001
(https://www.ibm.com/support/fixcentral/swg/selectFixes?product=ibm%2FTivoli%2FIBM+Tivoli+Key+Lifecycle+Manager&fixids=5.1.0-ISS-GKLM-FP0001&source=SAR&function=fixId&parent=IBM%20Security)</td></tr>
<tr><td>IBM Guardium Key Lifecycle Manager (GKLM) v4.1.1</td></tr>
<tr><td>IBM Guardium Key Lifecycle Manager (GKLM) v4.2</td></tr>
<tr><td>IBM Guardium Key Lifecycle Manager (GKLM) v4.2.1</td></tr>
<tr><td>IBM Guardium Key Lifecycle Manager (GKLM) v5.0</td><td></td></tr>
<tr><td>IBM Guardium Key Lifecycle Manager (GKLM) v5.1</td><td>Apply 5.1.0-ISS-GKLM-FP0001
(https://www.ibm.com/support/fixcentral/swg/selectFixes?product=ibm%2FTivoli%2FIBM+Tivoli+Key+Lifecycle+Manager&fixids=5.1.0-ISS-GKLM-FP0001&source=SAR&function=fixId&parent=IBM%20Security)</td></tr>
</table>

Download instruction - https://www.ibm.com/docs/en/gklm/5.x?topic=software-download-instructions

(https://www.ibm.com/docs/en/gklm/5.x?topic=software-download-instructions)

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)*

Change History

*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.

Document Information

More support for:

IBM Guardium Key Lifecycle Manager *(https://www.ibm.com/mysupport/s/topic/0TO5000000025yUGAQ)*

Software version:

4.1, 4.1.1, 4.2, 4.2.1, 5.0, 5.1

Operating system(s):

AIX, Windows, Linux

Document number:

7268697

Modified date:

07 April 2026