



CVE-2021-38983

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-38983
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-15 16:15:00 UTC
Updated	2021-11-16 19:23:00 UTC
Description	IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 uses weaker than expected cryptographic algorithms that could al

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	ibm	Aix	-	All	All	All
Application	ibm	Security Guardium Key Lifecycle Manager	4.1.0	All	All	All
Application	ibm	Security Guardium Key Lifecycle Manager	4.1.0.1	All	All	All
Application	ibm	Security Guardium Key Lifecycle Manager	4.1.1	All	All	All
Application	ibm	Security Key Lifecycle Manager	4.1.0	All	All	All
Application	ibm	Security Key Lifecycle Manager	4.1.0.1	All	All	All
Application	ibm	Security Key Lifecycle Manager	4.1.1	All	All	All
Application	ibm	Security Key Lifecycle Manager	All	All	All	All
Application	ibm	Security Key Lifecycle Manager	All	All	All	All
Application	ibm	Security Key Lifecycle Manager	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

References

Reference	Source	Link
Security Bulletin: Inadequate encryption strength in IBM Security Guardium Key Lifecycle Manager (CVE-2021-38983)	CONFIRM	www.ibm.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com

CVE Program record

CVE.ORG www.cve.org

NVD vulnerability detail

NVD nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report