



# CVE-2021-38979

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

## Summary

<b>CVE</b>	CVE-2021-38979
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@us.ibm.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-11-15 16:15:00 UTC
<b>Updated</b>	2022-07-12 17:42:00 UTC
<b>Description</b>	IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0, and 4.1 uses a one-way cryptographic hash against an input that should n

## Risk And Classification

**Problem Types:** CWE-916

## 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	Li
IBM X-Force Exchange	XF	e:
Security Bulletin: Use of a one way hash without a salt in IBM Security Guardium Key Lifecycle Manager (CVE-2021-38979)	CONFIRM	w

CVE Program record

CVE.ORG [w](#)

NVD vulnerability detail

NVD [n](#)

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](#)