CVE-2021-38979

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-38979
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	2022-07-12 17:42:00 UTC
Description	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	ex
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	nv

No vendor comments have been submitted for this CVE.

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