CVE-2018-1745

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

Summary

CVE	CVE-2018-1745
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-11 12:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	IBM Security Key Lifecycle Manager 2.7 and 3.0 could allow an unauthenticated user to restart the SKLM server due to mis

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Security Key Lifecycle Manager	All	All	All	All
Application	Ibm	Security Key Lifecycle Manager	All	All	All	All

References

Reference	Source	Link
IBM Security Key Lifecycle Manager CVE-2018-1745 Remote Denial of Service Vulnerability	BID	www.secu
Security Bulletin: IBM Security Key Lifecycle Manager Misses Authentication for Critical Function (CVE-2018-1745)	CONFIRM	www.ibm.c
IBM X-Force Exchange	XF	exchange.
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

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 registred 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