



CVE-2017-12819

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

Summary

CVE	CVE-2017-12819
State	PUBLIC
Assigner	vulnerability@kaspersky.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-04 01:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Remote manipulations with language pack updater lead to NTLM-relay attack for system user in Gemalto's HASP SRM, Se

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Sentinel	Sentinel Ldk Rte Firmware	All	All	All	All

References

Reference
Siemens Building Technologies Products (Update A) CISA
KLCERT-17-005: Sentinel LDK RTE: Remote manipulations with language pack updater lead to NTLM-relay attack for system user Kaspersk
cert-portal.siemens.com/productcert/pdf/ssa-727467.pdf
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[590561](#) GE Common Licensing Multiple Vulnerabilities (GED SecComm 18-02)

[590593](#) GE Common Licensing Multiple Vulnerabilities (GED SecComm 18-02)

© [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](#)