



CVE-2017-11497

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

Summary

CVE	CVE-2017-11497
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-03 01:29:00 UTC
Updated	2018-05-11 01:29:00 UTC
Description	Stack buffer overflow in hasplms in Gemalto ACC (Admin Control Center), all versions ranging from HASP SRM 2.10 to Ser

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gemalto	Sentinel Ldk Rte	2.10	All	All	All
Application	Gemalto	Sentinel Ldk Rte	3.0	All	All	All
Application	Gemalto	Sentinel Ldk Rte	7.1	All	All	All
Application	Gemalto	Sentinel Ldk Rte	7.50	All	All	All
Application	Gemalto	Sentinel Ldk Rte	2.10	All	All	All
Application	Gemalto	Sentinel Ldk Rte	3.0	All	All	All
Application	Gemalto	Sentinel Ldk Rte	7.1	All	All	All
Application	Gemalto	Sentinel Ldk Rte	7.50	All	All	All

References

Reference
Siemens Building Technologies Products (Update A) CISA
www.iotvillage.org/slides_dc25/Sergey_Vlad_DEFCON_IOT_Village_Public2017.pptx
Gemalto Sentinel License Manager Multiple Security Vulnerabilities
Siemens SIMATIC WinCC Add-On ICS-CERT
KLCERT-17-002: Sentinel LDK RTE: language packs containing malformed filenames lead to Remote Code Execution Kaspersky ICS CERT
Multiple Siemens SIMATIC WinCC Add-On Products Multiple Security Vulnerabilities

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