CVE-2016-4407

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

Summary

CVE	CVE-2016-4407
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-13 14:59:00 UTC
Updated	2016-11-28 20:17:00 UTC
Description	The DSA algorithm implementation in SAP SAPCRYPTOLIB 5.555.38 does not properly check signatures, which allows rer

Risk And Classification

Problem Types: CWE-284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Sapcryptolib	5.555.38	All	All	All
Application	Sap	Sapcryptolib	5.555.38	All	All	All

References

Reference	Source	Link
SAP Missing Signature Check in DSA Algorithm | Onapsis	MISC	www.onapsi
Full Disclosure: Onapsis Security Advisory ONAPSIS-2016-029: SAP Missing Signature Check in DSA Algorithm	FULLDISC	seclists.org
SAP SAPCRYPTOLIB Component CVE-2016-4407 Security Bypass Vulnerability	BID	www.securit
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report