CVE-2018-16868

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

Summary

CVE	CVE-2018-16868
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-03 14:29:00 UTC
Updated	2022-11-30 21:20:00 UTC
Description	A Bleichenbacher type side-channel based padding oracle attack was found in the way gnutls handles verification of RSA d

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Gnutls	All	All	All	All

References

Reference
[security-announce] openSUSE-SU-2019:1353-1: important: Security update
1654929 – (CVE-2018-16868) CVE-2018-16868 gnutls: Bleichenbacher-like side channel leakage in PKCS#1 v1.5 verification and padding or
Your browser does not support frames. We recommend upgrading your browser.
[security-announce] openSUSE-SU-2019:1477-1: important: Security update
GNU GnuTLS CVE-2018-16868 Information Disclosure Vulnerability
CVE Program record
NVD vulnerability detail

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