CVE-2018-16869

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-16869
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-03 14:29:00 UTC
Updated	2023-02-03 14:25:00 UTC
Description	A Bleichenbacher type side-channel based padding oracle attack was found in the way nettle handles endian conversion of

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nettle Project	Nettle	All	All	All	All

References

Reference	Source	Link
GNU Nettle CVE-2018-16869 Information Disclosure Vulnerability	BID	www.securityfocus.
1654930 – (CVE-2018-16869) CVE-2018-16869 nettle: Leaky data conversion exposing a manager oracle	CONFIRM	bugzilla.redhat.com
Your browser does not support frames. We recommend upgrading your browser.	MISC	cat.eyalro.net
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

198408 Ubuntu Security Notification for Nettle vulnerabilities (USN-4990-1)

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