CVE-2016-1551

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

Summary

CVE	CVE-2016-1551
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-27 17:59:00 UTC
Updated	2017-11-21 02:29:00 UTC
Description	ntpd in NTP 4.2.8p3 and NTPsec a5fb34b9cc89b92a8fef2f459004865c93bb7f92 relies on the underlying operating system

Risk And Classification

Problem Types: CWE-254

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ntp	Ntp	4.2.8	p3	All	All
Application	Ntp	Ntp	4.2.8	p3	All	All
Application	Ntpsec	Ntpsec	a5fb34b9cc89b92a8fef2f459004865c93bb7f92	All	All	All
Application	Ntpsec	Ntpsec	a5fb34b9cc89b92a8fef2f459004865c93bb7f92	All	All	All

References

Reference
NTP CVE-2016-1551 Remote Security Vulnerability
Oracle Solaris Bulletin - April 2016
NTP: Multiple vulnerabilities (GLSA 201607-15) — Gentoo Security
April 2016 Network Time Protocol Daemon (ntpd) Vulnerabilities in Multiple NetApp Products | NetApp Product Security
ntp Multiple Bugs Let Remote Users Spoof Messages, Obtain Potentially Sensitive Information, Modify Time, and Deny Service - SecurityTrac
Cisco Talos - Talos 2016 0132
FreeBSD-SA-16:16
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**