CVE-2015-5146

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

Summary

CVE	CVE-2015-5146
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-24 20:29:00 UTC
Updated	2018-08-02 01:29:00 UTC
Description	ntpd in ntp before 4.2.8p3 with remote configuration enabled allows remote authenticated users with knowledge of the confi

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Application	Ntp	Ntp	All	p2	All	All

References

Reference
[SECURITY] Fedora 22 Update: ntp-4.2.6p5-33.fc22
support.ntp.org/bin/view/Main/SecurityNotice
Debian -- Security Information -- DSA-3388-1 ntp

NTP CVE-2015-5146 Denial of Service Vulnerability
CVE-2015-5146 Network Time Protocol Daemon (ntpd) Denial of Service Vulnerability in NetApp Products | NetApp Product Security
Gentoo Security
Bug 2853 – Crafted remote config packet can crash some versions of ntpd.
Ntpd Remote Configuration Bug Lets Remote Authenticated Users on the Local Network Cause the Target Service to Crash - SecurityTracker
1238136 – (CVE-2015-5146) CVE-2015-5146 ntp: ntpd control message crash on crafted NUL-byte in configuration directive (VU#668167)
[SECURITY] Fedora 21 Update: ntp-4.2.6p5-34.fc21
[SECURITY] Fedora 23 Update: ntp-4.2.6p5-33.fc23
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**