CVE-2015-7853

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-7853
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-07 20:29:00 UTC
Updated	2021-07-16 13:15:00 UTC
Description	The datalen parameter in the refclock driver in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Netapp	Clustered Data Ontap	-	All	All	All
Operating System	Netapp	Clustered Data Ontap	-	All	All	All
Operating System	Netapp	Data Ontap	-	All	All	All
Operating System	Netapp	Data Ontap	-	All	All	All
Application	Netapp	Oncommand Balance	-	All	All	All
Application	Netapp	Oncommand Balance	-	All	All	All
Application	Netapp	Oncommand Performance Manager	-	All	All	All
Application	Netapp	Oncommand Performance Manager	-	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Application	Ntp	Ntp	All	All	All	All
Application	Ntp	Ntp	4.2.8	-	All	All
Application	Ntp	Ntp	4.2.8	p1	All	All
Application	Ntp	Ntp	4.2.8	p1-beta1	All	All
Application	Ntp	Ntp	4.2.8	p1-beta2	All	All
Application	Ntp	Ntp	4.2.8	p1-beta3	All	All
Application	Ntp	Ntp	4.2.8	p1-beta4	All	All

Application	Ntp	Ntp	4.2.8	p1-beta5	All	All
Application	Ntp	Ntp	4.2.8	p1-rc1	All	All
Application	Ntp	Ntp	4.2.8	p1-rc2	All	All
Application	Ntp	Ntp	4.2.8	p2	All	All
Application	Ntp	Ntp	4.2.8	p2-rc1	All	All
Application	Ntp	Ntp	4.2.8	p2-rc2	All	All
Application	Ntp	Ntp	4.2.8	p2-rc3	All	All
Application	Ntp	Ntp	4.2.8	p3	All	All
Application	Ntp	Ntp	4.2.8	p3-rc1	All	All
Application	Ntp	Ntp	4.2.8	p3-rc2	All	All
Application	Ntp	Ntp	4.2.8	p3-rc3	All	All
Application	Ntp	Ntp	All	All	All	All
Application	Ntp	Ntp	4.2.8	-	All	All
Application	Ntp	Ntp	4.2.8	p1	All	All
Application	Ntp	Ntp	4.2.8	p1-beta1	All	All
Application	Ntp	Ntp	4.2.8	p1-beta2	All	All
Application	Ntp	Ntp	4.2.8	p1-beta3	All	All
Application	Ntp	Ntp	4.2.8	p1-beta4	All	All
Application	Ntp	Ntp	4.2.8	p1-beta5	All	All
Application	Ntp	Ntp	4.2.8	p1-rc1	All	All
Application	Ntp	Ntp	4.2.8	p1-rc2	All	All
Application	Ntp	Ntp	4.2.8	p2	All	All
Application	Ntp	Ntp	4.2.8	p2-rc1	All	All
Application	Ntp	Ntp	4.2.8	p2-rc2	All	All
Application	Ntp	Ntp	4.2.8	p2-rc3	All	All
Application	Ntp	Ntp	4.2.8	p3	All	All
Application	Ntp	Ntp	4.2.8	p3-rc1	All	All
Application	Ntp	Ntp	4.2.8	p3-rc2	All	All
Application	Ntp	Ntp	4.2.8	p3-rc3	All	All

References

Reference	Source
[security-announce] SUSE-SU-2016:1247-1: important: Security update for	SUSE
USN-2783-1: NTP vulnerabilities | Ubuntu	UBUNTU
Siemens SIMATIC NET CP 443-1 OPC UA | CISA	MISC

SecurityFocus	BUGTRAQ
NTP: Multiple vulnerabilities (GLSA 201607-15) — Gentoo Security	GENTOO
SecurityFocus	BUGTRAQ
October 2015 Network Time Protocol Daemon (ntpd) Vulnerabilities in Multiple NetApp Products | NetApp Product Security	CONFIRM
1274262 – (CVE-2015-7853) CVE-2015-7853 ntp: reference clock memory corruption vulnerability	CONFIRM
cert-portal.siemens.com/productcert/pdf/ssa-211752.pdf	CONFIRM
openSUSE-SU-2016:1423-1: moderate: Security update for ntp	SUSE
openSUSE-SU-2015:2016-1: moderate: Security update for ntp	SUSE
Broadcom Support Portal	CONFIRM
Network Time Protocol CVE-2015-7853 Local Buffer Overflow Vulnerability	BID
SecurityFocus	BUGTRAQ
ntp Multiple Flaws Let Remote Users Deny Service, View Files, and Bypass Authentication to Modify the Time - SecurityTracker	SECTRACI
support.ntp.org/bin/view/Main/NtpBug2920	CONFIRM
[security-announce] SUSE-SU-2016:1311-1: important: Security update for	SUSE
SecurityFocus	BUGTRAQ
Cisco Talos - Vulnerability Reports	MISC
[security-announce] SUSE-SU-2016:1912-1: important: Security update for	SUSE
Slackware Security Advisory - ntp Updates ≈ Packet Storm	MISC
SecurityFocus	BUGTRAQ
FreeBSD Security Advisory - ntp Authentication Bypass ≈ Packet Storm	MISC
SecurityFocus	BUGTRAQ
[security-announce] SUSE-SU-2016:2094-1: important: Security update for	SUSE
SecurityFocus	BUGTRAQ
SecurityFocus	BUGTRAQ
Multiple Vulnerabilities in ntpd Affecting Cisco Products - October 2015	CISCO
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

590349 Rockwell Automation Stratix 5900 Multiple Vulnerabilities (ICSA-17-094-04)

590736 Siemens SIMATIC NET CP 443-1 OPC UA Multiple Vulnerabilities (ICSA-21-159-11)

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