CVE-2015-7871

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-7871
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-07 20:29:00 UTC
Updated	2021-04-13 12:15:00 UTC
Description	Crypto-NAK packets in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to bypass authen

Risk And Classification

Problem Types: CWE-287

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	9.0	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	Debian	Debian Linux	9.0	All	All	All
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	4.2.5	p186	All	All
Application	Ntp	Ntp	4.2.5	p187	All	All
Application	Ntp	Ntp	4.2.5	p188	All	All
Application	Ntp	Ntp	4.2.5	p189	All	All
Application	Ntp	Ntp	4.2.5	p190	All	All
Application	Ntp	Ntp	4.2.5	p191	All	All
Application	Ntp	Ntp	4.2.5	p192	All	All
Application	Ntp	Ntp	4.2.5	p193	All	All
Application	Ntp	Ntp	4.2.5	p194	All	All
Application	Ntp	Ntp	4.2.5	p195	All	All
Application	Ntp	Ntp	4.2.5	p196	All	All
Application	Ntp	Ntp	4.2.5	p197	All	All
Application	Ntp	Ntp	4.2.5	p198	All	All
Application	Ntp	Ntp	4.2.5	p199	All	All
Application	Ntp	Ntp	4.2.5	p200	All	All
Application	Ntp	Ntp	4.2.5	p201	All	All
Application	Ntp	Ntp	4.2.5	p202	All	All
Application	Ntp	Ntp	4.2.5	p203	All	All
Application	Ntp	Ntp	4.2.5	p204	All	All
Application	Ntp	Ntp	4.2.5	p205	All	All
Application	Ntp	Ntp	4.2.5	p206	All	All
Application	Ntp	Ntp	4.2.5	p207	All	All
Application	Ntp	Ntp	4.2.5	p208	All	All
Application	Ntp	Ntp	4.2.5	p209	All	All
Application	Ntp	Ntp	4.2.5	p210	All	All
Application	Ntp	Ntp	4.2.5	p211	All	All
Application	Ntp	Ntp	4.2.5	p212	All	All
Application	Ntp	Ntp	4.2.5	p213	All	All
Application	Ntp	Ntp	4.2.5	p214	All	All
Application	Ntp	Ntp	4.2.5	p215	All	All
Application	Ntp	Ntp	4.2.5	p216	All	All
Application	Ntp	Ntp	4.2.5	p217	All	All
Application	Ntp	Ntp	4.2.5	p218	All	All
Application	Ntp	Ntp	4.2.5	p219	All	All
Application	Ntp	Ntp	4.2.5	p220	All	All

Application	Ntp	Ntp	4.2.5	p221	All	All
Application	Ntp	Ntp	4.2.5	p222	All	All
Application	Ntp	Ntp	4.2.5	p223	All	All
Application	Ntp	Ntp	4.2.5	p224	All	All
Application	Ntp	Ntp	4.2.5	p225	All	All
Application	Ntp	Ntp	4.2.5	p226	All	All
Application	Ntp	Ntp	4.2.5	p227	All	All
Application	Ntp	Ntp	4.2.5	p228	All	All
Application	Ntp	Ntp	4.2.5	p229	All	All
Application	Ntp	Ntp	4.2.5	p230	All	All
Application	Ntp	Ntp	4.2.5	p231_rc1	All	All
Application	Ntp	Ntp	4.2.5	p232_rc1	All	All
Application	Ntp	Ntp	4.2.5	p233_rc1	All	All
Application	Ntp	Ntp	4.2.5	p234_rc1	All	All
Application	Ntp	Ntp	4.2.5	p235_rc1	All	All
Application	Ntp	Ntp	4.2.5	p236_rc1	All	All
Application	Ntp	Ntp	4.2.5	p237_rc1	All	All
Application	Ntp	Ntp	4.2.5	p238_rc1	All	All
Application	Ntp	Ntp	4.2.5	p239_rc1	All	All
Application	Ntp	Ntp	4.2.5	p240_rc1	All	All
Application	Ntp	Ntp	4.2.5	p241_rc1	All	All
Application	Ntp	Ntp	4.2.5	p242_rc1	All	All
Application	Ntp	Ntp	4.2.5	p243_rc1	All	All
Application	Ntp	Ntp	4.2.5	p244_rc1	All	All
Application	Ntp	Ntp	4.2.5	p245_rc1	All	All
Application	Ntp	Ntp	4.2.5	p246_rc1	All	All
Application	Ntp	Ntp	4.2.5	p247_rc1	All	All
Application	Ntp	Ntp	4.2.5	p248_rc1	All	All
Application	Ntp	Ntp	4.2.5	p249_rc1	All	All
Application	Ntp	Ntp	4.2.5	p250_rc1	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	4.2.5	p186	All	All
Application	Ntp	Ntp	4.2.5	p187	All	All
Application	Ntp	Ntp	4.2.5	p188	All	All
Application	Ntp	Ntp	4.2.5	p189	All	All
Application	Ntp	Ntp	4.2.5	p190	All	All
Application	Ntp	Ntp	4.2.5	p191	All	All
Application	Ntp	Ntp	4.2.5	p192	All	All
Application	Ntp	Ntp	4.2.5	p193	All	All
Application	Ntp	Ntp	4.2.5	p194	All	All
Application	Ntp	Ntp	4.2.5	p195	All	All
Application	Ntp	Ntp	4.2.5	p196	All	All
Application	Ntp	Ntp	4.2.5	p197	All	All
Application	Ntp	Ntp	4.2.5	p198	All	All
Application	Ntp	Ntp	4.2.5	p199	All	All
Application	Ntp	Ntp	4.2.5	p200	All	All
Application	Ntp	Ntp	4.2.5	p201	All	All
Application	Ntp	Ntp	4.2.5	p202	All	All
Application	Ntp	Ntp	4.2.5	p203	All	All
Application	Ntp	Ntp	4.2.5	p204	All	All
Application	Ntp	Ntp	4.2.5	p205	All	All
Application	Ntp	Ntp	4.2.5	p206	All	All
Application	Ntp	Ntp	4.2.5	p207	All	All
Application	Ntp	Ntp	4.2.5	p208	All	All
Application	Ntp	Ntp	4.2.5	p209	All	All

Application	Ntp	Ntp	4.2.5	p210	All	All
Application	Ntp	Ntp	4.2.5	p211	All	All
Application	Ntp	Ntp	4.2.5	p212	All	All
Application	Ntp	Ntp	4.2.5	p213	All	All
Application	Ntp	Ntp	4.2.5	p214	All	All
Application	Ntp	Ntp	4.2.5	p215	All	All
Application	Ntp	Ntp	4.2.5	p216	All	All
Application	Ntp	Ntp	4.2.5	p217	All	All
Application	Ntp	Ntp	4.2.5	p218	All	All
Application	Ntp	Ntp	4.2.5	p219	All	All
Application	Ntp	Ntp	4.2.5	p220	All	All
Application	Ntp	Ntp	4.2.5	p221	All	All
Application	Ntp	Ntp	4.2.5	p222	All	All
Application	Ntp	Ntp	4.2.5	p223	All	All
Application	Ntp	Ntp	4.2.5	p224	All	All
Application	Ntp	Ntp	4.2.5	p225	All	All
Application	Ntp	Ntp	4.2.5	p226	All	All
Application	Ntp	Ntp	4.2.5	p227	All	All
Application	Ntp	Ntp	4.2.5	p228	All	All
Application	Ntp	Ntp	4.2.5	p229	All	All
Application	Ntp	Ntp	4.2.5	p230	All	All
Application	Ntp	Ntp	4.2.5	p231_rc1	All	All
Application	Ntp	Ntp	4.2.5	p232_rc1	All	All
Application	Ntp	Ntp	4.2.5	p233_rc1	All	All
Application	Ntp	Ntp	4.2.5	p234_rc1	All	All
Application	Ntp	Ntp	4.2.5	p235_rc1	All	All
Application	Ntp	Ntp	4.2.5	p236_rc1	All	All
Application	Ntp	Ntp	4.2.5	p237_rc1	All	All
Application	Ntp	Ntp	4.2.5	p238_rc1	All	All
Application	Ntp	Ntp	4.2.5	p239_rc1	All	All
Application	Ntp	Ntp	4.2.5	p240_rc1	All	All
Application	Ntp	Ntp	4.2.5	p241_rc1	All	All
Application	Ntp	Ntp	4.2.5	p242_rc1	All	All
Application	Ntp	Ntp	4.2.5	p243_rc1	All	All
Application	Ntp	Ntp	4.2.5	p244_rc1	All	All

Application	Ntp	Ntp	4.2.5	p245_rc1	All	All
Application	Ntp	Ntp	4.2.5	p246_rc1	All	All
Application	Ntp	Ntp	4.2.5	p247_rc1	All	All
Application	Ntp	Ntp	4.2.5	p248_rc1	All	All
Application	Ntp	Ntp	4.2.5	p249_rc1	All	All
Application	Ntp	Ntp	4.2.5	p250_rc1	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
support.ntp.org/bin/view/Main/NtpBug2941	CONFIRM
NTP: Multiple vulnerabilities (GLSA 201607-15) — Gentoo Security	GENTOO
October 2015 Network Time Protocol Daemon (ntpd) Vulnerabilities in Multiple NetApp Products | NetApp Product Security	CONFIRM
Debian -- Security Information -- DSA-3388-1 ntp	DEBIAN
ntp Multiple Flaws Let Remote Users Deny Service, View Files, and Bypass Authentication to Modify the Time - SecurityTracker	SECTRAC
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security	GENTOO
Network Time Protocol CVE-2015-7871 Authentication Bypass Vulnerability	BID
Document Display | HPE Support Center	CONFIRM
cert-portal.siemens.com/productcert/pdf/ssa-497656.pdf	CONFIRM
1274265 – (CVE-2015-7871) CVE-2015-7871 ntp: crypto-NAK symmetric association authentication bypass vulnerability	CONFIRM
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)

590721 Siemens TIM 4R-IE Devices Multiple Vulnerabilities (ICSA-21-103-11)