



CVE-2017-6455

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2017-6455
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-27 17:59:00 UTC
Updated	2017-10-24 01:29:00 UTC
Description	NTP before 4.2.8p10 and 4.3.x before 4.3.94, when using PPSAPI, allows local users to gain privileges via a DLL in the PP

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ntp	Ntp	4.2.8	p9	All	All
Application	Ntp	Ntp	4.3.0	All	All	All
Application	Ntp	Ntp	4.3.1	All	All	All
Application	Ntp	Ntp	4.3.10	All	All	All
Application	Ntp	Ntp	4.3.11	All	All	All
Application	Ntp	Ntp	4.3.12	All	All	All
Application	Ntp	Ntp	4.3.13	All	All	All
Application	Ntp	Ntp	4.3.14	All	All	All
Application	Ntp	Ntp	4.3.15	All	All	All
Application	Ntp	Ntp	4.3.16	All	All	All
Application	Ntp	Ntp	4.3.17	All	All	All
Application	Ntp	Ntp	4.3.18	All	All	All
Application	Ntp	Ntp	4.3.19	All	All	All
Application	Ntp	Ntp	4.3.2	All	All	All
Application	Ntp	Ntp	4.3.20	All	All	All
Application	Ntp	Ntp	4.3.21	All	All	All
Application	Ntp	Ntp	4.3.22	All	All	All

Application	Ntp	Ntp	4.3.23	All	All	All
Application	Ntp	Ntp	4.3.24	All	All	All
Application	Ntp	Ntp	4.3.25	All	All	All
Application	Ntp	Ntp	4.3.26	All	All	All
Application	Ntp	Ntp	4.3.27	All	All	All
Application	Ntp	Ntp	4.3.28	All	All	All
Application	Ntp	Ntp	4.3.29	All	All	All
Application	Ntp	Ntp	4.3.3	All	All	All
Application	Ntp	Ntp	4.3.30	All	All	All
Application	Ntp	Ntp	4.3.31	All	All	All
Application	Ntp	Ntp	4.3.32	All	All	All
Application	Ntp	Ntp	4.3.33	All	All	All
Application	Ntp	Ntp	4.3.34	All	All	All
Application	Ntp	Ntp	4.3.35	All	All	All
Application	Ntp	Ntp	4.3.36	All	All	All
Application	Ntp	Ntp	4.3.37	All	All	All
Application	Ntp	Ntp	4.3.38	All	All	All
Application	Ntp	Ntp	4.3.39	All	All	All
Application	Ntp	Ntp	4.3.4	All	All	All
Application	Ntp	Ntp	4.3.40	All	All	All
Application	Ntp	Ntp	4.3.41	All	All	All
Application	Ntp	Ntp	4.3.42	All	All	All
Application	Ntp	Ntp	4.3.43	All	All	All
Application	Ntp	Ntp	4.3.44	All	All	All
Application	Ntp	Ntp	4.3.45	All	All	All
Application	Ntp	Ntp	4.3.46	All	All	All
Application	Ntp	Ntp	4.3.47	All	All	All
Application	Ntp	Ntp	4.3.48	All	All	All
Application	Ntp	Ntp	4.3.49	All	All	All
Application	Ntp	Ntp	4.3.5	All	All	All
Application	Ntp	Ntp	4.3.50	All	All	All
Application	Ntp	Ntp	4.3.51	All	All	All
Application	Ntp	Ntp	4.3.52	All	All	All
Application	Ntp	Ntp	4.3.53	All	All	All
Application	Ntp	Ntp	4.3.54	All	All	All

Application	Ntp	Ntp	4.3.55	All	All	All
Application	Ntp	Ntp	4.3.56	All	All	All
Application	Ntp	Ntp	4.3.57	All	All	All
Application	Ntp	Ntp	4.3.58	All	All	All
Application	Ntp	Ntp	4.3.59	All	All	All
Application	Ntp	Ntp	4.3.6	All	All	All
Application	Ntp	Ntp	4.3.60	All	All	All
Application	Ntp	Ntp	4.3.61	All	All	All
Application	Ntp	Ntp	4.3.62	All	All	All
Application	Ntp	Ntp	4.3.63	All	All	All
Application	Ntp	Ntp	4.3.64	All	All	All
Application	Ntp	Ntp	4.3.65	All	All	All
Application	Ntp	Ntp	4.3.66	All	All	All
Application	Ntp	Ntp	4.3.67	All	All	All
Application	Ntp	Ntp	4.3.68	All	All	All
Application	Ntp	Ntp	4.3.69	All	All	All
Application	Ntp	Ntp	4.3.7	All	All	All
Application	Ntp	Ntp	4.3.70	All	All	All
Application	Ntp	Ntp	4.3.71	All	All	All
Application	Ntp	Ntp	4.3.72	All	All	All
Application	Ntp	Ntp	4.3.73	All	All	All
Application	Ntp	Ntp	4.3.74	All	All	All
Application	Ntp	Ntp	4.3.75	All	All	All
Application	Ntp	Ntp	4.3.76	All	All	All
Application	Ntp	Ntp	4.3.77	All	All	All
Application	Ntp	Ntp	4.3.78	All	All	All
Application	Ntp	Ntp	4.3.79	All	All	All
Application	Ntp	Ntp	4.3.8	All	All	All
Application	Ntp	Ntp	4.3.80	All	All	All
Application	Ntp	Ntp	4.3.81	All	All	All
Application	Ntp	Ntp	4.3.82	All	All	All
Application	Ntp	Ntp	4.3.83	All	All	All
Application	Ntp	Ntp	4.3.84	All	All	All
Application	Ntp	Ntp	4.3.85	All	All	All
Application	Ntp	Ntp	4.3.86	All	All	All
Application	Ntp	Ntp	4.3.87	All	All	All

Application	Ntp	Ntp	4.3.87	All	All	All
Application	Ntp	Ntp	4.3.88	All	All	All
Application	Ntp	Ntp	4.3.89	All	All	All
Application	Ntp	Ntp	4.3.9	All	All	All
Application	Ntp	Ntp	4.3.90	All	All	All
Application	Ntp	Ntp	4.3.91	All	All	All
Application	Ntp	Ntp	4.3.92	All	All	All
Application	Ntp	Ntp	4.3.93	All	All	All
Application	Ntp	Ntp	4.2.8	p9	All	All
Application	Ntp	Ntp	4.3.0	All	All	All
Application	Ntp	Ntp	4.3.1	All	All	All
Application	Ntp	Ntp	4.3.10	All	All	All
Application	Ntp	Ntp	4.3.11	All	All	All
Application	Ntp	Ntp	4.3.12	All	All	All
Application	Ntp	Ntp	4.3.13	All	All	All
Application	Ntp	Ntp	4.3.14	All	All	All
Application	Ntp	Ntp	4.3.15	All	All	All
Application	Ntp	Ntp	4.3.16	All	All	All
Application	Ntp	Ntp	4.3.17	All	All	All
Application	Ntp	Ntp	4.3.18	All	All	All
Application	Ntp	Ntp	4.3.19	All	All	All
Application	Ntp	Ntp	4.3.2	All	All	All
Application	Ntp	Ntp	4.3.20	All	All	All
Application	Ntp	Ntp	4.3.21	All	All	All
Application	Ntp	Ntp	4.3.22	All	All	All
Application	Ntp	Ntp	4.3.23	All	All	All
Application	Ntp	Ntp	4.3.24	All	All	All
Application	Ntp	Ntp	4.3.25	All	All	All
Application	Ntp	Ntp	4.3.26	All	All	All
Application	Ntp	Ntp	4.3.27	All	All	All
Application	Ntp	Ntp	4.3.28	All	All	All
Application	Ntp	Ntp	4.3.29	All	All	All
Application	Ntp	Ntp	4.3.3	All	All	All
Application	Ntp	Ntp	4.3.30	All	All	All
Application	Ntp	Ntp	4.3.31	All	All	All
Application	Ntp	Ntp	4.3.32	All	All	All

Application	Ntp	Ntp	4.3.33	All	All	All
Application	Ntp	Ntp	4.3.34	All	All	All
Application	Ntp	Ntp	4.3.35	All	All	All
Application	Ntp	Ntp	4.3.36	All	All	All
Application	Ntp	Ntp	4.3.37	All	All	All
Application	Ntp	Ntp	4.3.38	All	All	All
Application	Ntp	Ntp	4.3.39	All	All	All
Application	Ntp	Ntp	4.3.4	All	All	All
Application	Ntp	Ntp	4.3.40	All	All	All
Application	Ntp	Ntp	4.3.41	All	All	All
Application	Ntp	Ntp	4.3.42	All	All	All
Application	Ntp	Ntp	4.3.43	All	All	All
Application	Ntp	Ntp	4.3.44	All	All	All
Application	Ntp	Ntp	4.3.45	All	All	All
Application	Ntp	Ntp	4.3.46	All	All	All
Application	Ntp	Ntp	4.3.47	All	All	All
Application	Ntp	Ntp	4.3.48	All	All	All
Application	Ntp	Ntp	4.3.49	All	All	All
Application	Ntp	Ntp	4.3.5	All	All	All
Application	Ntp	Ntp	4.3.50	All	All	All
Application	Ntp	Ntp	4.3.51	All	All	All
Application	Ntp	Ntp	4.3.52	All	All	All
Application	Ntp	Ntp	4.3.53	All	All	All
Application	Ntp	Ntp	4.3.54	All	All	All
Application	Ntp	Ntp	4.3.55	All	All	All
Application	Ntp	Ntp	4.3.56	All	All	All
Application	Ntp	Ntp	4.3.57	All	All	All
Application	Ntp	Ntp	4.3.58	All	All	All
Application	Ntp	Ntp	4.3.59	All	All	All
Application	Ntp	Ntp	4.3.6	All	All	All
Application	Ntp	Ntp	4.3.60	All	All	All
Application	Ntp	Ntp	4.3.61	All	All	All
Application	Ntp	Ntp	4.3.62	All	All	All
Application	Ntp	Ntp	4.3.63	All	All	All
Application	Ntp	Ntp	4.3.64	All	All	All

Application	Ntp	Ntp	4.3.65	All	All	All
Application	Ntp	Ntp	4.3.66	All	All	All
Application	Ntp	Ntp	4.3.67	All	All	All
Application	Ntp	Ntp	4.3.68	All	All	All
Application	Ntp	Ntp	4.3.69	All	All	All
Application	Ntp	Ntp	4.3.7	All	All	All
Application	Ntp	Ntp	4.3.70	All	All	All
Application	Ntp	Ntp	4.3.71	All	All	All
Application	Ntp	Ntp	4.3.72	All	All	All
Application	Ntp	Ntp	4.3.73	All	All	All
Application	Ntp	Ntp	4.3.74	All	All	All
Application	Ntp	Ntp	4.3.75	All	All	All
Application	Ntp	Ntp	4.3.76	All	All	All
Application	Ntp	Ntp	4.3.77	All	All	All
Application	Ntp	Ntp	4.3.78	All	All	All
Application	Ntp	Ntp	4.3.79	All	All	All
Application	Ntp	Ntp	4.3.8	All	All	All
Application	Ntp	Ntp	4.3.80	All	All	All
Application	Ntp	Ntp	4.3.81	All	All	All
Application	Ntp	Ntp	4.3.82	All	All	All
Application	Ntp	Ntp	4.3.83	All	All	All
Application	Ntp	Ntp	4.3.84	All	All	All
Application	Ntp	Ntp	4.3.85	All	All	All
Application	Ntp	Ntp	4.3.86	All	All	All
Application	Ntp	Ntp	4.3.87	All	All	All
Application	Ntp	Ntp	4.3.88	All	All	All
Application	Ntp	Ntp	4.3.89	All	All	All
Application	Ntp	Ntp	4.3.9	All	All	All
Application	Ntp	Ntp	4.3.90	All	All	All
Application	Ntp	Ntp	4.3.91	All	All	All
Application	Ntp	Ntp	4.3.92	All	All	All
Application	Ntp	Ntp	4.3.93	All	All	All

References

Reference

support.ntp.org/bin/view/Main/SecurityNotice

About the security content of macOS High Sierra 10.13 - Apple Support

support.ntp.org/bin/view/Main/NtpBug3384

NTP CVE-2017-6455 Local Denial of Service Vulnerability

ntp Multiple Bugs Let Remote or Local Users Cause the Target Service to Crash - SecurityTracker

Apple macOS/OS X Multiple Flaws Let Remote and Local Users Bypass Security and Deny Service, Local Users Obtain Potentially Sensitive

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[44030 Juniper Network Operating System \(Junos OS\) Multiple NTP Vulnerabilities \(JSA11171\)](#)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)