CVE-2010-0294

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

Summary

CVE	CVE-2010-0294
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-02-08 20:30:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	chronyd in Chrony before 1.23.1, and possibly 1.24-pre1, generates a syslog message for each unauthorized cmdmon pacl

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tuxfamily	Chrony	1.18	All	All	All

Application	Tuxfamily	Chrony	1.19	All	All	All
Application	Tuxfamily	Chrony	1.19-1	All	All	All
Application	Tuxfamily	Chrony	1.19.99.1	All	All	All
Application	Tuxfamily	Chrony	1.19.99.2	All	All	All
Application	Tuxfamily	Chrony	1.19.99.3	All	All	All
Application	Tuxfamily	Chrony	1.20	All	All	All
Application	Tuxfamily	Chrony	1.21	All	All	All
Application	Tuxfamily	Chrony	1.21-pre1	All	All	All
Application	Tuxfamily	Chrony	1.24-pre1	All	All	All
Application	Tuxfamily	Chrony	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
cgit error
Chrony
Debian -- Security Information -- DSA-1992-1 chrony
Chrony Denial of Service Security Issue and Vulnerability - Advisories - Community
Debian update for chrony - Advisories - Community
Chrony 1.23 and Prior Multiple Remote Denial of Service Vulnerabilities
555367 – (CVE-2010-0292, CVE-2010-0293, CVE-2010-0294) CVE-2010-0292 chrony susceptible to DoS attacks (CVE-2010-0293 CVE-201
cgit error
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**