CVE-2015-1821

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

Summary

CVE	CVE-2015-1821
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-16 14:59:00 UTC
Updated	2023-02-13 00:47:00 UTC
Description	Heap-based buffer overflow in chrony before 1.31.1 allows remote authenticated users to cause a denial of service (chrony

Risk And Classification

Problem Types: CWE-119

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	7.0	All	All	All
Application	Tuxfamily	Chrony	All	All	All	All

References

Reference	Source	Link	Tags
[chrony-announce] chrony-1.31.1 released (security)	MLIST	listengine.tuxfamily.org	Patch
Red Hat Customer Portal	MISC	access.redhat.com	
Chrony CVE-2015-1821 Out of Bounds Write Heap Buffer Overflow Vulnerability	BID	www.securityfocus.com	
Gentoo Security	GENTOO	security.gentoo.org	
1209631 – (CVE-2015-1821) CVE-2015-1821 chrony: Heap out of bound write in address filter	MISC	bugzilla.redhat.com	
Debian -- Security Information -- DSA-3222-1 chrony	DEBIAN	www.debian.org	
Oracle Linux Bulletin - October 2015	CONFIRM	www.oracle.com	
access.redhat.com | CVE-2015-1821	MISC	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

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**