CVE-2013-2178

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

Summary

CVE	CVE-2013-2178
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-08-28 23:55:10 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The apache-auth.conf, apache-nohome.conf, apache-noscript.conf, and apache-overflows.conf files in Fail2ban before 0.8.

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-20 | 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	Fail2ban	Fail2ban	0.1.0	All	All	All

Application	Fail2ban	Fail2ban	0.1.1	All	All	All
Application	Fail2ban	Fail2ban	0.1.2	All	All	All
Application	Fail2ban	Fail2ban	0.3.0	All	All	All
Application	Fail2ban	Fail2ban	0.3.1	All	All	All
Application	Fail2ban	Fail2ban	0.4.0	All	All	All
Application	Fail2ban	Fail2ban	0.4.1	All	All	All
Application	Fail2ban	Fail2ban	0.5.0	All	All	All
Application	Fail2ban	Fail2ban	0.5.1	All	All	All
Application	Fail2ban	Fail2ban	0.5.2	All	All	All
Application	Fail2ban	Fail2ban	0.5.3	All	All	All
Application	Fail2ban	Fail2ban	0.5.4	All	All	All
Application	Fail2ban	Fail2ban	0.5.5	All	All	All
Application	Fail2ban	Fail2ban	0.6.0	All	All	All
Application	Fail2ban	Fail2ban	0.6.1	All	All	All
Application	Fail2ban	Fail2ban	0.7.0	All	All	All
Application	Fail2ban	Fail2ban	0.7.1	All	All	All
Application	Fail2ban	Fail2ban	0.7.2	All	All	All
Application	Fail2ban	Fail2ban	0.7.3	All	All	All
Application	Fail2ban	Fail2ban	0.7.4	All	All	All
Application	Fail2ban	Fail2ban	0.7.5	All	All	All
Application	Fail2ban	Fail2ban	0.7.6	All	All	All
Application	Fail2ban	Fail2ban	0.7.7	All	All	All
Application	Fail2ban	Fail2ban	0.7.8	All	All	All
Application	Fail2ban	Fail2ban	0.7.9	All	All	All
Application	Fail2ban	Fail2ban	0.8.0	All	All	All
Application	Fail2ban	Fail2ban	0.8.1	All	All	All
Application	Fail2ban	Fail2ban	0.8.2	All	All	All
Application	Fail2ban	Fail2ban	0.8.3	All	All	All
Application	Fail2ban	Fail2ban	0.8.4	All	All	All
Application	Fail2ban	Fail2ban	0.8.5	All	All	All
Application	Fail2ban	Fail2ban	0.8.6	All	All	All
Application	Fail2ban	Fail2ban	0.8.7	All	All	All
Application	Fail2ban	Fail2ban	0.8.7.1	All	All	All
Application	Fail2ban	Fail2ban	0.8.8	All	All	All
Application	Fail2ban	Fail2ban	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecurity.o
openSUSE-SU-2014:0348-1: moderate: fail2ban: security and bugfix upgrade	af854a3a-2127-422b-91ae-364da2661108	lists.opensuse.o
raw.github.com/fail2ban/fail2ban/master/ChangeLog	af854a3a-2127-422b-91ae-364da2661108	raw.github.com
vndh.net/note:fail2ban-089-denial-service	af854a3a-2127-422b-91ae-364da2661108	vndh.net
Debian -- Security Information -- DSA-2708-1 fail2ban	af854a3a-2127-422b-91ae-364da2661108	www.debian.org
oss-security - Re: Re: Fail2ban 0.8.9, Denial of Service (Apache rules only)	af854a3a-2127-422b-91ae-364da2661108	www.openwall.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.