CVE-2013-7176

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

Summary

CVE	CVE-2013-7176
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-01 15:55:00 UTC
Updated	2014-11-19 02:59:00 UTC
Description	config/filter.d/postfix.conf in the postfix filter in Fail2ban before 0.8.11 allows remote attackers to trigger the blocking of an a

Risk And Classification

Problem Types: CWE-20

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	0.8.9	All	All	All
Application	Fail2ban	Fail2ban	All	All	All	All
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	0.8.9	All	All	All

References

Reference	Source	Link
openSUSE-SU-2014:0348-1: moderate: fail2ban: security and bugfix upgrade	SUSE	lists.opensuse.o
ENH: Improve postfix regex and add more samples · fail2ban/fail2ban@eb2f0c9 · GitHub	CONFIRM	github.com
Vulnerability Note VU#686662 - Fail2ban postfix and cyrus-imap filters contain denial-of-service vulnerabilities	CERT-VN	www.kb.cert.org
Debian -- Security Information -- DSA-2979-1 fail2ban	DEBIAN	www.debian.org
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report