CVE-2012-5642

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

Summary

CVE	CVE-2012-5642
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-12-31 11:50:27 UTC
Updated	2026-04-29 01:13:23 UTC
Description	server/action.py in Fail2ban before 0.8.8 does not properly handle the content of the matches tag, which might allow remote

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/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	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
Support / Security / Advisories / / MDVSA-2013:078 | Mandriva	af854a3a-2127-422b-91ae-3
BF: escape the content of <matches> since its value could contain arb… · fail2ban/fail2ban@83109bc · GitHub	af854a3a-2127-422b-91ae-3
openSUSE-SU-2013:0566-1: fail2ban: fixed a startup and security issue	af854a3a-2127-422b-91ae-3
447572 – (CVE-2012-5642) <net-analyzer/fail2ban-0.8.8: input variable quoting vulnerability (CVE-2012-5642)	af854a3a-2127-422b-91ae-3
openSUSE-SU-2013:0567-1: fail2ban: fixed a startup and security issue	af854a3a-2127-422b-91ae-3
raw.github.com/fail2ban/fail2ban/master/ChangeLog	af854a3a-2127-422b-91ae-3
oss-security - Re: CVE request: fail2ban 0.8.8 fixes an input variable quoting flaw on <matches> content	af854a3a-2127-422b-91ae-3
Fail2Ban / Mailing Lists	af854a3a-2127-422b-91ae-3
887914 – (CVE-2012-5642) CVE-2012-5642 fail2ban: does not escape the content of <matches>	af854a3a-2127-422b-91ae-3
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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