CVE-2015-8125

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

Summary

CVE	CVE-2015-8125
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-07 20:59:15 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Symfony 2.3.x before 2.3.35, 2.6.x before 2.6.12, and 2.7.x before 2.7.7 might allow remote attackers to have unspecified ir

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	Sensiolabs	Symfony	2.3.0	All	All	All

Application	Sensiolabs	Symfony	2.3.1	All	All	All
Application	Sensiolabs	Symfony	2.3.10	All	All	All
Application	Sensiolabs	Symfony	2.3.11	All	All	All
Application	Sensiolabs	Symfony	2.3.12	All	All	All
Application	Sensiolabs	Symfony	2.3.13	All	All	All
Application	Sensiolabs	Symfony	2.3.14	All	All	All
Application	Sensiolabs	Symfony	2.3.15	All	All	All
Application	Sensiolabs	Symfony	2.3.16	All	All	All
Application	Sensiolabs	Symfony	2.3.17	All	All	All
Application	Sensiolabs	Symfony	2.3.18	All	All	All
Application	Sensiolabs	Symfony	2.3.19	All	All	All
Application	Sensiolabs	Symfony	2.3.2	All	All	All
Application	Sensiolabs	Symfony	2.3.20	All	All	All
Application	Sensiolabs	Symfony	2.3.21	All	All	All
Application	Sensiolabs	Symfony	2.3.22	All	All	All
Application	Sensiolabs	Symfony	2.3.23	All	All	All
Application	Sensiolabs	Symfony	2.3.24	All	All	All
Application	Sensiolabs	Symfony	2.3.25	All	All	All
Application	Sensiolabs	Symfony	2.3.26	All	All	All
Application	Sensiolabs	Symfony	2.3.27	All	All	All
Application	Sensiolabs	Symfony	2.3.28	All	All	All
Application	Sensiolabs	Symfony	2.3.29	All	All	All
Application	Sensiolabs	Symfony	2.3.3	All	All	All
Application	Sensiolabs	Symfony	2.3.30	All	All	All
Application	Sensiolabs	Symfony	2.3.31	All	All	All
Application	Sensiolabs	Symfony	2.3.32	All	All	All
Application	Sensiolabs	Symfony	2.3.33	All	All	All
Application	Sensiolabs	Symfony	2.3.34	All	All	All
Application	Sensiolabs	Symfony	2.3.4	All	All	All
Application	Sensiolabs	Symfony	2.3.5	All	All	All
Application	Sensiolabs	Symfony	2.3.6	All	All	All
Application	Sensiolabs	Symfony	2.3.7	All	All	All
Application	Sensiolabs	Symfony	2.3.8	All	All	All
Application	Sensiolabs	Symfony	2.3.9	All	All	All
Application	Sensiolabs	Symfony	2.6.0	All	All	All
Application	Sensiolabs	Symfony	2.6.1	All	All	All

Application	Sensiolabs	Symfony	2.6.10	All	All	All
Application	Sensiolabs	Symfony	2.6.11	All	All	All
Application	Sensiolabs	Symfony	2.6.2	All	All	All
Application	Sensiolabs	Symfony	2.6.3	All	All	All
Application	Sensiolabs	Symfony	2.6.4	All	All	All
Application	Sensiolabs	Symfony	2.6.5	All	All	All
Application	Sensiolabs	Symfony	2.6.6	All	All	All
Application	Sensiolabs	Symfony	2.6.7	All	All	All
Application	Sensiolabs	Symfony	2.6.8	All	All	All
Application	Sensiolabs	Symfony	2.6.9	All	All	All
Application	Sensiolabs	Symfony	2.7.0	All	All	All
Application	Sensiolabs	Symfony	2.7.1	All	All	All
Application	Sensiolabs	Symfony	2.7.2	All	All	All
Application	Sensiolabs	Symfony	2.7.3	All	All	All
Application	Sensiolabs	Symfony	2.7.4	All	All	All
Application	Sensiolabs	Symfony	2.7.5	All	All	All
Application	Sensiolabs	Symfony	2.7.6	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Debian -- Security Information -- DSA-3402-1 symfony	af854a3a-2127-422b-91a
[SECURITY] Fedora 22 Update: php-twig-1.23.1-2.fc22	af854a3a-2127-422b-91a
[SECURITY] Fedora 23 Update: php-twig-1.23.1-2.fc23	af854a3a-2127-422b-91a
CVE-2015-8125: Potential Remote Timing Attack Vulnerability in Security Remember-Me Service (Symfony Blog)	af854a3a-2127-422b-91a
Malformed Request	af854a3a-2127-422b-91a
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.

Free CVE JSON API cve.report/api

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