CVE-2013-6440

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

Summary

CVE	CVE-2013-6440
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-14 15:55:05 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The (1) BasicParserPool, (2) StaticBasicParserPool, (3) XML Decrypter, and (4) SAML Decrypter in Shibboleth OpenSAML

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

EPSS: 0.007500000 probability, percentile 0.732840000 (date 2026-05-13)

Problem Types: CWE-200 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Internet2	Opensaml	2.0	All	All	All
Application	Internet2	Opensaml	2.1.0	All	All	All
Application	Internet2	Opensaml	2.2.0	All	All	All
Application	Shibboleth	Opensaml	2.4.0	All	All	All
Application	Shibboleth	Opensaml	2.4.1	All	All	All
Application	Shibboleth	Opensaml	2.4.2	All	All	All
Application	Shibboleth	Opensaml	2.4.3	All	All	All
Application	Shibboleth	Opensaml	2.5.0	All	All	All
Application	Shibboleth	Opensaml	2.5.1	All	All	All
Application	Shibboleth	Opensaml	2.5.2	All	All	All
Application	Shibboleth	Opensaml	2.5.3	All	All	All
Application	Shibboleth	Opensaml	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
Red Hat Customer Portal
Red Hat Customer Portal
Oracle Critical Patch Update Advisory - January 2022
1043332 – (CVE-2013-6440) CVE-2013-6440 XMLTooling-J/OpenSAML Java: XML eXternal Entity (XXE) flaw in ParserPool and Decrypter
shibboleth.net/community/advisories/secadv_20131213.txt
Red Hat Customer Portal
Red Hat Customer Portal
Web-based Single Sign-On and the Dangers of SAML XML Parsing - SendSafely
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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