CVE-2014-8080

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

Summary

CVE	CVE-2014-8080
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-03 16:55:07 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The REXML parser in Ruby 1.9.x before 1.9.3-p550, 2.0.x before 2.0.0-p594, and 2.1.x before 2.1.4 allows remote attacker

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: NVD-CWE-Other | 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
Operating System	Canonical	Ubuntu Linux	12.04	-	lts	All

Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Ruby-lang	Ruby	1.9.3	All	All	All
Application	Ruby-lang	Ruby	1.9.3	p0	All	All
Application	Ruby-lang	Ruby	1.9.3	p125	All	All
Application	Ruby-lang	Ruby	1.9.3	p194	All	All
Application	Ruby-lang	Ruby	1.9.3	p286	All	All
Application	Ruby-lang	Ruby	1.9.3	p383	All	All
Application	Ruby-lang	Ruby	1.9.3	p385	All	All
Application	Ruby-lang	Ruby	1.9.3	p392	All	All
Application	Ruby-lang	Ruby	1.9.3	p426	All	All
Application	Ruby-lang	Ruby	1.9.3	p429	All	All
Application	Ruby-lang	Ruby	1.9.3	p448	All	All
Application	Ruby-lang	Ruby	1.9.3	p545	All	All
Application	Ruby-lang	Ruby	1.9.3	p547	All	All
Application	Ruby-lang	Ruby	2.0.0	All	All	All
Application	Ruby-lang	Ruby	2.0.0	p0	All	All
Application	Ruby-lang	Ruby	2.0.0	p195	All	All
Application	Ruby-lang	Ruby	2.0.0	p247	All	All
Application	Ruby-lang	Ruby	2.0.0	p451	All	All
Application	Ruby-lang	Ruby	2.0.0	p481	All	All
Application	Ruby-lang	Ruby	2.0.0	p576	All	All
Application	Ruby-lang	Ruby	2.1.1	All	All	All
Application	Ruby-lang	Ruby	2.1.2	All	All	All
Application	Ruby-lang	Ruby	2.1.3	All	All	All
Application	Ruby-lang	Ruby	All	p550	All	All

Vendor Declared Affected Products

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

References

Reference	Source

Reference	Source
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364
Security Advisory SA61607 - Ruby REXML XML Entity Expansion Denial of Service Vulnerability - Secunia	af854a3a-2127-422b-91ae-364
Security Advisory SA62748 - SUSE update for ruby - Secunia	af854a3a-2127-422b-91ae-364
Debian -- Security Information -- DSA-3159-1 ruby1.8	af854a3a-2127-422b-91ae-364
APPLE-SA-2015-09-30-3 OS X El Capitan 10.11	af854a3a-2127-422b-91ae-364
CVE-2014-8080: Denial of Service XML Expansion	af854a3a-2127-422b-91ae-364
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364
USN-2397-1: Ruby vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364
Mageia Advisory: MGASA-2014-0443 - Updated ruby packages fix CVE-2014-8080	af854a3a-2127-422b-91ae-364
Security Advisory SA62050 - SUSE update for ruby20 - Secunia	af854a3a-2127-422b-91ae-364
Oracle Linux Bulletin - January 2016	af854a3a-2127-422b-91ae-364
openSUSE-SU-2014:1589-1: moderate: Security update for ruby19	af854a3a-2127-422b-91ae-364
openSUSE-SU-2015:0007-1: moderate: Security update for ruby2.1	af854a3a-2127-422b-91ae-364
Ruby CVE-2014-8080 XML External Entity Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364
Support / Security / Advisories / / MDVSA-2015:129 | Mandriva	af854a3a-2127-422b-91ae-364
About the security content of OS X El Capitan v10.11 - Apple Support	af854a3a-2127-422b-91ae-364
openSUSE-SU-2015:0002-1: moderate: Security update for ruby20	af854a3a-2127-422b-91ae-364
Debian -- Security Information -- DSA-3157-1 ruby1.9.1	af854a3a-2127-422b-91ae-364
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.