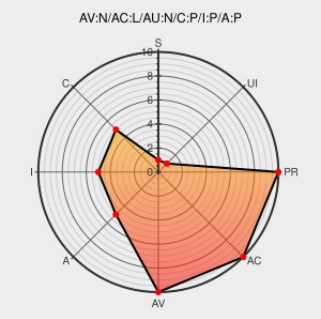
CVE-2013-1802

Published on: 04/09/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:14 AM UTC

CVE-2013-1802

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Extlib from Dan Kubb contain the following vulnerability:

The extlib gem 0.9.15 and earlier for Ruby does not properly restrict casts of string values, which might allow remote attackers to conduct object-injection attacks and execute arbitrary code, or cause a denial of service (memory and CPU consumption) by leveraging Action Pack support for (1) YAML type conversion or (2) Symbol type conversion, a similar vulnerability to CVE-2013-0156.

CVE-2013-1802 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
January 14, 2013: Security vulnerabilities: httparty, extlib, crack, nori: Update these gems immediately : Engine Yard Developer Center	support.cloud.engineyard.com text/html	MISC gems-imr
[security-announce] SUSE-SU-2013:0612-1: important: Security update for	lists.opensuse.org text/html	SUSE
917233 – (CVE-2013-1802) CVE-2013-1802 rubygem-extlib: YAML parameter parsing vulnerability	bugzilla.redhat.com text/html	MISC
Comparing b4f98174ec35ac96f76a08d5624fad05d22879b5...4540e7102b803624cc2eade4bb8aaaa934fc31c5 · datamapper/extlib · GitHub	Exploit Patch github.com text/html	CONF github.co

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dan Kubb	Extlib	0.9.10	All	All	All
Application	Dan Kubb	Extlib	0.9.11	All	All	All
Application	Dan Kubb	Extlib	0.9.12	All	All	All
Application	Dan Kubb	Extlib	0.9.13	All	All	All
Application	Dan Kubb	Extlib	0.9.14	All	All	All
Application	Dan Kubb	Extlib	0.9.2	All	All	All
Application	Dan Kubb	Extlib	0.9.3	All	All	All
Application	Dan Kubb	Extlib	0.9.4	All	All	All
Application	Dan Kubb	Extlib	0.9.5	All	All	All
Application	Dan Kubb	Extlib	0.9.6	All	All	All
Application	Dan Kubb	Extlib	0.9.7	All	All	All
Application	Dan Kubb	Extlib	0.9.8	All	All	All
Application	Dan Kubb	Extlib	0.9.9	All	All	All
Application	Dan Kubb	Extlib	All	All	All	All
Application	Dan Kubb	Extlib	0.9.10	All	All	All
Application	Dan Kubb	Extlib	0.9.11	All	All	All
Application	Dan Kubb	Extlib	0.9.12	All	All	All
Application	Dan Kubb	Extlib	0.9.13	All	All	All
Application	Dan Kubb	Extlib	0.9.14	All	All	All
Application	Dan Kubb	Extlib	0.9.2	All	All	All
Application	Dan Kubb	Extlib	0.9.3	All	All	All
Application	Dan Kubb	Extlib	0.9.4	All	All	All
Application	Dan Kubb	Extlib	0.9.5	All	All	All
Application	Dan Kubb	Extlib	0.9.6	All	All	All
Application	Dan Kubb	Extlib	0.9.7	All	All	All
Application	Dan Kubb	Extlib	0.9.8	All	All	All
Application	Dan Kubb	Extlib	0.9.9	All	All	All

cpe:2.3:a:dan_kubb:extlib:0.9.10:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.11:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.12:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.13:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.14:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.3:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.4:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.5:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.6:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.7:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.8:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.9:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:*:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.10:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.11:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.12:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.13:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.14:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.3:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.4:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.5:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.6:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.7:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.8:*:*:*:*:*:*:*:

cpe:2.3:a:dan_kubb:extlib:0.9.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→