CVE-2021-41816

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-41816
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-06 21:15:00 UTC
Updated	2024-01-24 05:15:00 UTC
Description	CGI.escape_html in Ruby before 2.7.5 and 3.x before 3.0.3 has an integer overflow and resultant buffer overflow via a long

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Ruby-lang	Cgi	All	All	All	All
Application	Ruby-lang	Cgi	All	All	All	All
Application	Ruby-lang	Cgi	All	All	All	All
Application	Ruby-lang	Ruby	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 35 Update: ruby-3.0.4-153.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
CVE-2021-41816 Ruby Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
[SECURITY] Fedora 35 Update: ruby-3.0.4-153.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 34 Update: ruby-3.0.4-153.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Ruby: Multiple vulnerabilities (GLSA 202401-27) — Gentoo security		security.gentoo.org
CVE-2021-41816: Buffer Overrun in CGI.escape_html	CONFIRM	www.ruby-lang.org
CVE-2021-41816	MISC	security-tracker.debian.org
HackerOne	MISC	hackerone.com

[SECURITY] Fedora 34 Update: ruby-3.0.4-153.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 179050 Debian Security Update for ruby2.7 (DSA 5067-1)
- 198635 Ubuntu Security Notification for Ruby Vulnerabilities (USN-5235-1)
- 240720 Red Hat Update for rh-ruby27-ruby security (RHSA-2022:6856)
- 240723 Red Hat Update for rh-ruby30-ruby security (RHSA-2022:6855)
- 282660 Fedora Security Update for ruby (FEDORA-2022-82a9edac27)
- 282661 Fedora Security Update for ruby (FEDORA-2022-8cf0124add)
- 356181 Amazon Linux Security Advisory for ruby : ALASRUBY3.0-2023-003
- 356463 Amazon Linux Security Advisory for ruby : ALAS2RUBY3.0-2023-003
- 500617 Alpine Linux Security Update for ruby
- 502024 Alpine Linux Security Update for ruby
- 504377 Alpine Linux Security Update for ruby
- 690621 Free Berkeley Software Distribution (FreeBSD) Security Update for rubygem-cgi (2c6af5c3-4d36-11ec-a539-0800270512f4)
- 710844 Gentoo Linux Ruby Multiple Vulnerabilities (GLSA 202401-27)
- 904903 Common Base Linux Mariner (CBL-Mariner) Security Update for ruby (12423)