



# CVE-2020-8164

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-8164
<b>State</b>	PUBLIC
<b>Assigner</b>	support@hackerone.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-19 17:15:00 UTC
<b>Updated</b>	2022-05-24 16:44:00 UTC
<b>Description</b>	A deserialization of untrusted data vulnerability exists in rails < 5.2.4.3, rails < 6.0.3.1 which can allow an attacker to supply

## Risk And Classification

**Problem Types:** CWE-502

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Opensuse</a>	<a href="#">Backports Sle</a>	15.0	sp1	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	All	All	All	All
Application	<a href="#">Rubyonrails</a>	<a href="#">Rails</a>	All	All	All	All

## References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2020:1575-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
[CVE-2020-8164] Possible Strong Parameters Bypass in ActionPack	MISC	<a href="https://groups.google.com">groups.google.com</a>	Patch, Third Party Advisory
HackerOne	MISC	<a href="https://hackerone.com">hackerone.com</a>	Exploit, Patch, Third Party
[security-announce] openSUSE-SU-2020:1533-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	

Debian -- Security Information -- DSA-4766-1 rails	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
[SECURITY] [DLA 2282-1] rails security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	Mailing List, Third Party Ad
[security-announce] openSUSE-SU-2020:1536-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
[SECURITY] [DLA 2251-1] rails security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	Mailing List, Third Party Ad
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [239228](#) Red Hat Update for Satellite 6.9 (RHSA-2021:1313)
- [750577](#) OpenSUSE Security Update for rmt-server (openSUSE-SU-2020:2000-1)
- [750580](#) OpenSUSE Security Update for rmt-server (openSUSE-SU-2020:1993-1)
- [750625](#) OpenSUSE Security Update for rubygem-actionpack-5\_1 (openSUSE-SU-2020:1536-1)
- [750628](#) OpenSUSE Security Update for rubygem-actionpack-5\_1 (openSUSE-SU-2020:1533-1)

© [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 registered 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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)