



# NRSS RSS Reader 0.3.9-1 Stack Buffer Overflow

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

## Summary

<b>CVE</b>	CVE-2016-20043
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-28 12:16:00 UTC
<b>Updated</b>	2026-04-10 20:59:49 UTC
<b>Description</b>	NRSS RSS Reader 0.3.9-1 contains a stack buffer overflow vulnerability that allows local attackers to execute arbitrary code

## Risk And Classification

**Primary CVSS:** v4.0 8.6 HIGH from disclosure@vulncheck.com

**CVSS:** 4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000150000 probability, percentile 0.031990000 (date 2026-04-15)

**Problem Types:** CWE-787 | CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	8.6	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA
4.0	CNA	CVSS	8.6	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	disclosure@vulncheck.com	Secondary	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nrss	Nrss	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platform
--------	--------	---------	---------	----------

Source	Vendor	Product	Version	Platforms
CNA	NrSS	NRSS Reader	affected 0.3.9	Not specified

## References

Reference	Source	Link	Tags
<a href="http://www.vulncheck.com/advisories/nrss-rss-reader-1-stack-buffer-overflow">www.vulncheck.com/advisories/nrss-rss-reader-1-stack-buffer-overflow</a>	disclosure@vulncheck.com	<a href="http://www.vulncheck.com">www.vulncheck.com</a>	Third Party Adv
<a href="http://www.exploit-db.com/exploits/39810">www.exploit-db.com/exploits/39810</a>	disclosure@vulncheck.com	<a href="http://www.exploit-db.com">www.exploit-db.com</a>	Exploit, VDB En
<a href="http://www.codezen.org/nrss">www.codezen.org/nrss</a>	disclosure@vulncheck.com	<a href="http://www.codezen.org">www.codezen.org</a>	Broken Link, Pr
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, anal

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Juan Sacco - <http://www.exploitpack.com> - [jsacco@exploitpack.com](mailto:jsacco@exploitpack.com) (en)

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 registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

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