



CVE-2015-7762

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

Summary

CVE	CVE-2015-7762
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-06 21:59:00 UTC
Updated	2016-12-07 18:25:00 UTC
Description	rx/rx.c in OpenAFS before 1.6.15 and 1.7.x before 1.7.33 does not properly initialize the padding of a data structure when c

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Openafs	Openafs	1.7.1	All	All	All
Application	Openafs	Openafs	1.7.10	All	All	All
Application	Openafs	Openafs	1.7.11	All	All	All
Application	Openafs	Openafs	1.7.12	All	All	All
Application	Openafs	Openafs	1.7.13	All	All	All
Application	Openafs	Openafs	1.7.14	All	All	All
Application	Openafs	Openafs	1.7.15	All	All	All
Application	Openafs	Openafs	1.7.16	All	All	All
Application	Openafs	Openafs	1.7.17	All	All	All
Application	Openafs	Openafs	1.7.18	All	All	All
Application	Openafs	Openafs	1.7.19	All	All	All
Application	Openafs	Openafs	1.7.2	All	All	All
Application	Openafs	Openafs	1.7.20	All	All	All

Application	Openafs	Openafs	1.7.21	All	All	All
Application	Openafs	Openafs	1.7.22	All	All	All
Application	Openafs	Openafs	1.7.23	All	All	All
Application	Openafs	Openafs	1.7.24	All	All	All
Application	Openafs	Openafs	1.7.25	All	All	All
Application	Openafs	Openafs	1.7.26	All	All	All
Application	Openafs	Openafs	1.7.27	All	All	All
Application	Openafs	Openafs	1.7.28	All	All	All
Application	Openafs	Openafs	1.7.29	All	All	All
Application	Openafs	Openafs	1.7.3	All	All	All
Application	Openafs	Openafs	1.7.30	All	All	All
Application	Openafs	Openafs	1.7.31	All	All	All
Application	Openafs	Openafs	1.7.4	All	All	All
Application	Openafs	Openafs	1.7.8	All	All	All
Application	Openafs	Openafs	1.7.1	All	All	All
Application	Openafs	Openafs	1.7.10	All	All	All
Application	Openafs	Openafs	1.7.11	All	All	All
Application	Openafs	Openafs	1.7.12	All	All	All
Application	Openafs	Openafs	1.7.13	All	All	All
Application	Openafs	Openafs	1.7.14	All	All	All
Application	Openafs	Openafs	1.7.15	All	All	All
Application	Openafs	Openafs	1.7.16	All	All	All
Application	Openafs	Openafs	1.7.17	All	All	All
Application	Openafs	Openafs	1.7.18	All	All	All
Application	Openafs	Openafs	1.7.19	All	All	All
Application	Openafs	Openafs	1.7.2	All	All	All
Application	Openafs	Openafs	1.7.20	All	All	All
Application	Openafs	Openafs	1.7.21	All	All	All
Application	Openafs	Openafs	1.7.22	All	All	All
Application	Openafs	Openafs	1.7.23	All	All	All
Application	Openafs	Openafs	1.7.24	All	All	All
Application	Openafs	Openafs	1.7.25	All	All	All
Application	Openafs	Openafs	1.7.26	All	All	All
Application	Openafs	Openafs	1.7.27	All	All	All
Application	Openafs	Openafs	1.7.28	All	All	All

Application	Openafs	Openafs	1.7.29	All	All	All
Application	Openafs	Openafs	1.7.3	All	All	All
Application	Openafs	Openafs	1.7.30	All	All	All
Application	Openafs	Openafs	1.7.31	All	All	All
Application	Openafs	Openafs	1.7.4	All	All	All
Application	Openafs	Openafs	1.7.8	All	All	All
Application	Openafs	Openafs	All	All	All	All

References

Reference

www.openafs.org/pages/security/OPENAFS-SA-2015-007.txt

OpenAFS Rx Protocol Packet Initialization Flaw Lets Remote Users Obtain Potentially Sensitive Plaintext Information on the Target System - S

Debian -- Security Information -- DSA-3387-1 openafs

[OpenAFS-announce] OpenAFS security release 1.6.15 available

www.openafs.org/dl/openafs/1.6.15/RELNOTES-1.6.15

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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](#) 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](#)