



CVE-2014-8886

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

Summary

CVE	CVE-2014-8886
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-08 20:59:00 UTC
Updated	2018-10-09 19:54:00 UTC
Description	AVM FRITZ!OS before 6.30 extracts the contents of firmware updates before verifying their cryptographic signature, which

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Avm	Fritz! Os	All	All	All	All
Operating System	Avm	Fritz! Os	All	All	All	All

References

Reference	Source	Link
RedTeam Pentesting GmbH - AVM FRITZ!Box: Arbitrary Code Execution Through Manipulated Firmware Images	MISC	www.re
Sicherheitsinfos zu Updates AVM Deutschland	CONFIRM	avm.de
SecurityFocus	BUGTRAQ	www.se
AVM FRITZ!Box: Arbitrary Code Execution Via Firmware Images ~ Packet Storm	MISC	packets
Full Disclosure: [RT-SA-2014-014] AVM FRITZ!Box: Arbitrary Code Execution Through Manipulated Firmware Images	FULLDISC	seclists
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nis

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](#).

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

CVE.report and Source URL Uptime Status [status.cve.report](#)