



CVE-2018-16852

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

Summary

CVE	CVE-2018-16852
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-28 14:29:00 UTC
Updated	2019-10-09 23:36:00 UTC
Description	Samba from version 4.9.0 and before version 4.9.3 is vulnerable to a NULL pointer de-reference. During the processing of a

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
Samba Security Bypass and Denial of Service Vulnerabilities	BID
Samba - Security Announcement Archive	CONFIRM
November 2018 Samba Vulnerabilities in NetApp StorageGRID Products NetApp Product Security	CONFIRM
Samba: Multiple vulnerabilities (GLSA 202003-52) — Gentoo security	GENTOO
1646386 – (CVE-2018-16852) CVE-2018-16852 samba: NULL pointer de-reference in Samba AD DC DNS management server	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)