

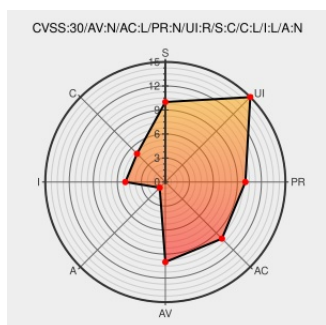


CVE-2018-1000528

Published on: 06/26/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:30 PM UTC

CVE-2018-1000528

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

GONICUS GOsa version before commit

56070d6289d47ba3f5918885954dcceb75606001 contains a Cross Site Scripting (XSS) vulnerability in change password form (html/password.php, #308) that can result in injection of arbitrary web script or HTML. This attack appear to be exploitable via the victim must open a specially crafted web page. This vulnerability appears to have been fixed in after commit 56070d6289d47ba3f5918885954dcceb75606001.

CVE-2018-1000528 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
(cve #11) goss project/goss cve@56070d6	CVE	MISC github.com/goss-project/goss

(see #14) · gosa-project/gosa-core@56070d6 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/gosa-project/gosa-core/commit/56070d6289d47ba3f5918885954dcceb75606001
[SECURITY] [DLA 1436-1] gosa security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180720 [SECURITY] [DLA 1436-1] gosa security update
Server-Side Reflected XSS via POST to /gosa/password.php · Issue #14 · gosa-project/gosa-core · GitHub	Third Party Advisory github.com text/html	MISC github.com/gosa-project/gosa-core/issues/14
Debian -- Security Information -- DSA-4239-1 gosa	Third Party Advisory www.debian.org Deprecated Link text/html	DEBIAN DSA-4239

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gonicus	Gosa	-	All	All	All
Application	Gonicus	Gosa	-	All	All	All
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:a:gonicus:gosa:-:*:*:*:*:*:						
cpe:2.3:a:gonicus:gosa:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

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](#)