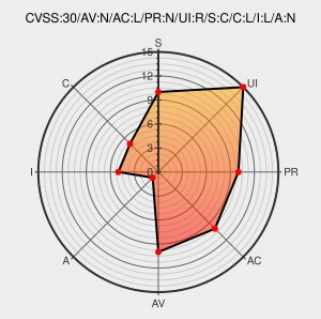
CVE-2018-1000528

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 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
(gosa #14) - gosa-project/gosa-core@56070d6	Patch	MISC:github.com/gosa-project/gosa

(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 Depreciated Link text/html	DEBIAN DSA-4239

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

← Previous ID

Next ID→