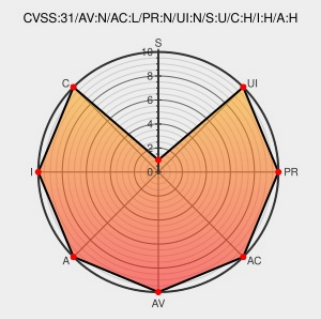
CVE-2019-15900

Published on: 10/18/2019 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-15900

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Doas from Doas Project contain the following vulnerability:

An issue was discovered in slicer69 doas before 6.2 on certain platforms other than OpenBSD. On platforms without strtonum(3), sscanf was used without checking for error cases. Instead, the uninitialized variable errstr was checked and in some cases returned success even if sscanf failed. The result was that, instead of reporting that the supplied username or group name did not exist, it would execute the command as root.

CVE-2019-15900 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Added optimization to Makefile	Patch	MISC

Added optimization to Makefile (can be set/overruled using OPT). · slicer69/doas@2f83222 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/slicer69/doas/commit/2f83222829448e5bc4c9391d607ec265a1e06531
Comparing 6.1p1...6.2 · slicer69/doas · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/slicer69/doas/compare/6.1p1...6.2

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
Application	Doas Project	Doas	All	All	All	All
Application	Doas Project	Doas	All	All	All	All

cpe:2.3:a:doas_project:doas:*:*:*:*:*:*:*:*:

cpe:2.3:a:doas_project:doas:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→