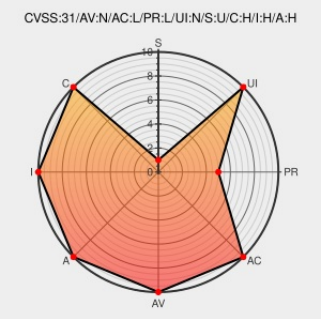
CVE-2019-25016

Published on: 01/28/2021 12:00:00 AM UTC

Last Modified on: 04/26/2022 04:14:00 PM UTC

CVE-2019-25016

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



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

In OpenDoas from 6.6 to 6.8 the users PATH variable was incorrectly inherited by authenticated executions if the authenticating rule allowed the user to execute any command. Rules that only allowed to authenticated user to execute specific commands were not affected by this issue.

CVE-2019-25016 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
redo the environment inheritance to not inherit. it was intended to m… · Duncaen/OpenDoas@01c658f	Patch Third Party Advisory github.com	MISC github.com/Duncaen/OpenDoas/commit/01c658f8c45cb92a343be5f32aa6da70b2032

Duncaen/OpenDoas@01c658f · GitHub	text/html	
OpenDoas: Insufficient environment filtering (GLSA 202107-11) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202107-11
OpenDoas keeps current PATH variable · Issue #45 · Duncaen/OpenDoas · GitHub	Exploit Issue Tracking Third Party Advisory github.com text/html	MISC github.com/Duncaen/OpenDoas/issues/45
Release v6.8.1: - This release fixes one major issue that has been assigned CVE-2019-… · Duncaen/OpenDoas · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/Duncaen/OpenDoas/releases/tag/v6.8.1
correctly reset path for rules without specific command · Duncaen/OpenDoas@d5acd52 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/Duncaen/OpenDoas/commit/d5acd52e2a15c36a8e06f9103d35622933aa4

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.

Related QID Numbers

500161 Alpine Linux Security Update for doas

501397 Alpine Linux Security Update for doas

710065 Gentoo Linux OpenDoas Insufficient environment filtering (GLSA 202107-11)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opendoas Project	Opendoas	All	All	All	All

cpe:2.3:a:opendoas_project:opendoas:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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