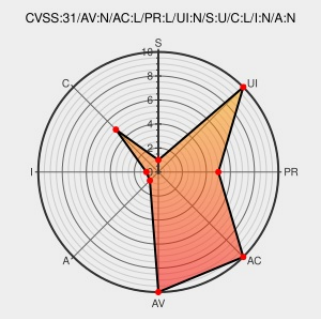
CVE-2022-38731

Published on: Not Yet Published

Last Modified on: 02/24/2023 06:14:00 PM UTC

CVE-2022-38731

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



Certain versions of Dose from Qaelum contain the following vulnerability:

Qaelum DOSE 18.08 through 21.1 before 21.2 allows Directory Traversal via the loadimages name parameter. It allows a user to specify an arbitrary location on the server's filesystem from which to load an image. (Only images are displayed to the attacker. All other files are loaded but not displayed.) The Content-Type response header reflects the actual content type of the file being requested. This allows an attacker to enumerate files on the local system. Additionally, remote resources can be requested via a UNC path, allowing an attacker to coerce authentication out from the server to the attackers machine.

CVE-2022-38731 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
How our Ethical Hacking team discovered a “zero-day” vulnerability - PwC UK	www.pwc.co.uk text/html	MISC www.pwc.co.uk/issues/cyber-security-services/research/ethical-hacking-team-discovered-zero-day-vulnerability.html
Qaelum - Dose	web.archive.org text/html Inactive Link Not Archived	MISC qaelum.com/solutions/dose

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

Exploit/POC from Github

Qaelum DOSE 18.08 through 21.1 before 21.2 allows Directory Traversal via the loadimages name parameter. It allows a …

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qaelum	Dose	All	All	All	All

cpe:2.3:a:qaelum:dose:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@cKure7	[redacted] CVE-2022-38731: A blind arbitrary file read, that could also be used for authentication coercion via a mechan… twitter.com/i/web/status/1…	2023-02-15 05:27:58
@CVEreport	CVE-2022-38731 : Qaelum DOSE 18.08 through 21.1 before 21.2 allows Directory Traversal via the loadimages name para… twitter.com/i/web/status/1…	2023-02-16 14:02:19
@threatmeter	CVE-2022-38731 | Qaelum DOSE up to 21.1 Response Header loadimages name path traversal A vulnerability, which was c… twitter.com/i/web/status/1…	2023-02-16 15:50:17
/r/netcve	CVE-2022-38731	2023-02-16 14:38:04

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report