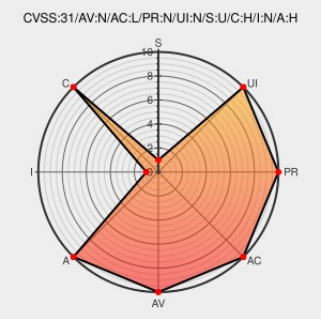
CVE-2020-29551

Published on: 12/23/2020 12:00:00 AM UTC

Last Modified on: 04/26/2022 04:12:00 PM UTC

CVE-2020-29551

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



Certain versions of Urve from Urve contain the following vulnerability:

An issue was discovered in URVE Build 24.03.2020. Using the _internal/pc/shutdown.php path, it is possible to shutdown the system. Among others, the following files and scripts are also accessible: _internal/pc/abort.php, _internal/pc/restart.php, _internal/pc/vpro.php, _internal/pc/wake.php, _internal/error_u201409.txt, _internal/runcmd.php, _internal/getConfiguration.php, ews/autoload.php, ews/del.php, ews/mod.php, ews/sync.php, utils/backup/backup_server.php, utils/backup/restore_server.php, MyScreens/timeline.config, kreator.html5/test.php, and addedlogs.txt.

CVE-2020-29551 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.1 - CRITICAL

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

CVSS2 Score: 8.5 - HIGH

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

CVE References

Description	Tags	Link

System rezerwacji sal z ekranem dotykowym - zarządzanie salami - LOBO	Vendor Advisory urve.co.uk text/html	MISC urve.co.uk/system-rezerwacji-sal
URVE Software Build 24.03.2020 Missing Authorization ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/160725/URVE-Software-Build-24.03.2020-Missing-Authorization.html
	Exploit Third Party Advisory www.syss.de text/plain Inactive Link Not Archived	MISC www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-041.txt
Full Disclosure: SYSS-2020-041 Urve - Missing Authorization (CWE-862)	seclists.org text/html	FULLDISC 20201225 SYSS-2020-041 Urve - Missing Authorization (CWE-862)

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	Urve	Urve	24.03.2020	All	All	All
Application	Urve	Urve	24.03.2020	All	All	All

cpe:2.3:a:urve:urve:24.03.2020:*:*:*:*:*:*:*:

cpe:2.3:a:urve:urve:24.03.2020:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→