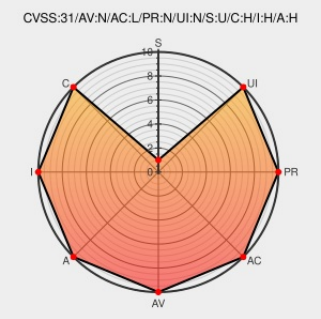
CVE-2020-29552

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

Last Modified on: 09/02/2022 03:47:00 AM UTC

CVE-2020-29552

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. By using the _internal/pc/vpro.php?mac=0&ip=0&operation=0&usr=0&pass=0%3bpowershell+-c+" substring, it is possible to execute a Powershell command and redirect its output to a file under the web root.

CVE-2020-29552 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
System rezerwacji sal z ekranem dotykowym - zarządzanie salami - LOBO	Vendor Advisory, urve.co.uk, text/html	MISC urve.co.uk/system-rezerwacji-sal
	Exploit	MISC

	Third Party Advisory www.syss.de text/plain	www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-040.txt
URVE Software Build 24.03.2020 Authentication Bypass / Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/160722/URVE-Software-Build-24.03.2020-Authentication-Bypass-Remote-Code-Execution.html
Full Disclosure: SYSS-2020-040 Urve - Missing Authentication for Critical Function (CWE-306)	seclists.org text/html	FULLDISC 20201225 SYSS-2020-040 Urve - Missing Authentication for Critical Function (CWE-306)

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

← Previous ID

Next ID→