

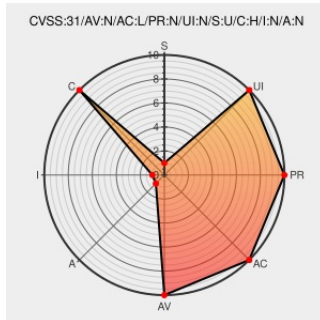


CVE-2020-29550

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

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

CVE-2020-29550

[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. The password of an integration user account (used for the connection of the MS Office 365 Integration Service) is stored in cleartext in configuration files as well as in the database. The following files contain the password in cleartext: Profiles/urve/files/sql_db.backup, Server/data/pg_wal/000000010000000A000000DD,

Server/data/base/16384/18617, and Server/data/base/17202/8708746. This causes the password to be displayed as cleartext in the HTML code as roomsreservationimport_password in /urve/roomsreservationimport/roomsreservationimport/update-HTML5.

CVE-2020-29550 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

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 Information Disclosure ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/160726/URVE-Software-Build-24.03.2020-Information-Disclosure.html
Full Disclosure: SYSS-2020-042 Urve - Exposure of Sensitive Information to an Unauthorized Actor (CWE-200)	seclists.org text/html	FULLDISC 20201225 SYSS-2020-042 Urve - Exposure of Sensitive Information to an Unauthorized Actor (CWE-200)
	Exploit Third Party Advisory www.syss.de text/plain	MISC www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-042.txt

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

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#)