Full Disclosure mailing list archives

List Archive Search

SYSS-2020-042 Urve - Exposure of Sensitive Information to an Unauthorized Actor (CWE-200)

From: Erik Steltzner <erik.steltzner () syss de>
Date: Wed, 23 Dec 2020 09:30:06 +0100

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Advisory ID:            SYSS-2020-042
Product:                URVE Software
Manufacturer:           Eveo Sp. z o.o.
Affected Version(s):    Build "24.03.2020"
Tested Version(s):      Build "24.03.2020"
Vulnerability Type:     Cleartext Storage of Sensitive Information
(CWE-312)
                        Exposure of Sensitive Information to an
Unauthorized Actor (CWE-200)
Risk Level:             High
Solution Status:        Open
Manufacturer Notification: 2020-11-10
Solution Date:          2020-11-18
Public Disclosure:      2020-12-23
CVE Reference:          CVE-2020-29550
Authors of Advisory:    Erik Steltzner, SySS GmbH
                        Christoph Ritter, SySS GmbH


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Overview:

URVE is a system for reserving rooms which also provides a web interface
with event scheduler.

The manufacturer describes the product as follows (see [1] and [2]):

'Booking rooms on touchscreen and easy integration with MS Exchange,
Lotus, Office 365, Google Calendar and other systems.
Great looking schedules right at the door.
Fight conference room theft with our 10" touchscreen wall-mounted
panel.'

'Manage displays, edit playlists and HTML5 content easily.
Our server can be installed on any Windows and works smoothly from
web browser.'

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Vulnerability Details:

The password of the user account which is used for the connection of
the MS Office 365 Integration Service is stored as plaintext in
configuration files, as well as in the database.

The following files contain the password in plaintext:

Profiles/urve/files/sql_db.backup
Server/data/pg_wal/000000010000000A000000DD
Server/data/base/16384/18617
Server/data/base/17202/8708746

This causes the password to be displayed as plaintext in the HTML code.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Proof of Concept (PoC):

The path
/urve/roomsreservationimport/roomsreservationimport/update-HTML5?id=<id>
contains the tag with the cleartext password:

<input id="roomsreservationimport_password" [...] value="clearTextPassword">

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Solution:

The password should be stored as cryptographic hash value.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Disclosure Timeline:

2020-10-28: Vulnerability discovered
2020-11-10: Vulnerability reported to manufacturer
2020-11-18: Patch released by manufacturer
2020-12-23: Public disclosure of vulnerability

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

References:

[1] Product Website for URVE
    https://urve.co.uk/system-rezerwacji-sal
[2] Product Website for URVE
    https://urve.co.uk
[3] SySS Security Advisory SYSS-2020-042

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-042.txt
[4] SySS Responsible Disclosure Policy
    https://www.syss.de/en/news/responsible-disclosure-policy/

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Credits:

This security vulnerability was found by Erik Steltzner and Christoph
Ritter of SySS GmbH.

E-Mail: erik.steltzner () syss de
Public Key:
https://www.syss.de/fileadmin/dokumente/PGPKeys/Erik_Steltzner.asc
Key ID: 0x4C7979CE53163268
Key Fingerprint: 6538 8216 555B FBE7 1E01 7FBD 4C79 79CE 5316 3268

E-Mail: christoph.ritter () syss de
Public Key:
```

~~~~~~

Disclaimer:

The information provided in this security advisory is provided "as is"
and without warranty of any kind. Details of this security advisory may
be updated in order to provide as accurate information as possible. The
latest version of this security advisory is available on the SySS website.

~~~~~~

Copyright:

Creative Commons - Attribution (by) - Version 3.0
URL: http://creativecommons.org/licenses/by/3.0/deed.en

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEZTiCF1Vb++ceAX+9TH15z1MWMmgFAl/i+1YACgkQTH15z1MW
Mmh3/Q//QN2YWirc8dEQCXpmkzQ36C2HB5QwkDyimYZ9cm6d0dOp0IoxqOTXTT0M
/SYxxwiAjsimZk5P5oM1Xz+H1Uqickvfy0rw3xg4XIrUBh5GY1FvD4+Jvfrj27Mv
NVRaqvMfVzkqvZvnVePxqMNekrJdBwIRyTVnQ9nCcFqTo6n3xeqprTw5shVRQtqW
7jbt1rznPjGRR6tKdGZW6e29MHBU6tCLm1Z+h5hI1yJgnItpwXKZc9D6cpcxutrp
yveyFlYOSsZ8Yy7a8mGtvkbsJZFbX9aFtxF7hCWousnEJo8fECS7BIbezQoqzl74
dnWwIU/ZzoQTThS14PhLk4fVV4tPbgg35EEdpoxhJiWbkMQGx6TJkz9t/+XDcu2R
JkqcMHZNV7XNJJLs+MPTg3TGXy5OKuiPbZpSnmT1NCowGTQbb4Ptt+EUGCiT5djA
oQSGwgWAGQN/hf+6mJp5VN6HvU1jitQ7UquDhaDYHR7/iI3HRM5e8piqpZvSVeqd
lspnsdVTDtsobumXOSdzWhh/J7e+m9DqsBFGkFVebE/uwkrowcScFTTWLK1v1fPT
aYlw40SXnLjRuSvLBe4KVR/7x1zLCPMz5OfnbE4vh8r+yDtxd5Q1dcSguzPV4bu5
lHBcV2E+jWPUk6zDQVT2vG1KTSgAGBRjKUf8DVQaTf2/aBMAJXw=
=YEPt
-----END PGP SIGNATURE-----

Attachment: OpenPGP_signature
Description: OpenPGP digital signature

← By Date → ← By Thread →

Current thread:

SYSS-2020-042 Urve - Exposure of Sensitive Information to an Unauthorized Actor (CWE-200) *Erik Steltzner (Dec 25)*

Site Search 🔍

Nmap Security Scanner

Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture

User's Guide
API docs
Download
Npcap OEM

Security Lists

Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools

Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About

About/Contact
Privacy
Advertising
Nmap Public Source License