URVE Software Build 24.03.2020 Information Disclosure

Authored by Erik Steltzner | Site syss.de

Posted Dec 27, 2020

URVE Software build version 24.03.2020 suffers from an information disclosure vulnerability that leaks passwords.

tags | exploit, info disclosure
advisories | CVE-2020-29550
SHA-256 | 6199f87d0e51f1396cb792820464ba5845e147f83c62285034cbbc37df02dd05

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
-----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:
https://www.syss.de/fileadmin/dokumente/PGPKeys/Christoph_Ritter.asc
Key ID: 0x05458E666D35EAE8
Key Fingerprint: 9FB0 1B9B 2F72 3DD5 3AF3 62D8 0545 8E66 6D35 EAE8

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

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.
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Copyright:

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

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

iQIzBAEBCgAdFiEEZTiCFlVb++ceAX+9TH15zlMWMmgFAl/i+lYACgkQTH15zlMW
Mmh3/Q//QN2YWircBdEQCXpmkzQ36C2HB5QwkDyimYZ9cm6d0dOp0IoxqOTXTT0M
/SYxxwiAjsimIk5P5oMlXz+HlUqickvfyOrw3xg4XIrUBh5GYlFvD4+Jvfrj27Mv
NVRaqvMfVzkgvZvnVePxqMNekrJdBwIRyTVnQ9nCcFqTo6n3xegprTw5shVRQtqW
7jbtlrznPjGRR6tKdGZW6e29MHBU6tCLmlZ+h5hIlyJgnItpWXEc9D6cpcxutrp
yveyFlYOSsZ8Yy7a8mGtvkbsJZFbX9aFtxF7hCWousnEJo8fECS7BIbezQoqzl74
dnWwIU/ZzoQTThS14PhLk4fVV4tPbgg35EEdpoxhJiWbkMQGx6TJkz9t/+XDcu2R
JkqcMHZNV7XNJJLs+MPTg3TGXy5OKuiPbZpSnmTlNCowGTQbb4Ptt+EUGCiT5djA
oQSGwgWAGQN/hf+6mJp5VN6HvUljitQ7UquDhaDYHR7/iI3HRM5e8piqpZvSVeqd
lspnsdVTDtsobumXOSdzWhh/J7e+m9DqsBFGkFVebE/uwkrowcScPTTWLK1vlfPT
aYlw4OSXnLjRuSvLBe4KVR/7xlzLCPMz5OfnbE4vhEr+yDtxd5QldcSguzPV4bu5
lHBcV2E+jWPUk6zDQVT2vGlKTSgAGBRjKUf8DVQaTf2/aBMAJXw=
=YEPt
-----END PGP SIGNATURE-----
```

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

packet storm

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed