SYSS-2020-041 Urve - Missing Authorization (CWE-862)

From: Erik Steltzner <erik.steltzner () syss de>
Date: Wed, 23 Dec 2020 09:29:57 +0100

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

Advisory ID:                SYSS-2020-041
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 Authorization (CWE-862)
Risk Level:                 High
Solution Status:            Open
Manufacturer Notification: 2020-11-10
Solution Date:              2020-11-18
Public Disclosure:          2020-12-23
CVE Reference:              CVE-2020-29551
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:

It is possible to access many different files without authentication in
an unauthorized way.

These files are partly PHP scripts which can potentially cause damage.

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

Proof of Concept (PoC):

Using the following path, it is possible to shut down the system:
_internal/pc/shutdown.php

Among others, the following files and scripts are also accessible:

_internal/pc/abort.php
_internal/pc/restart.php
_internal/pc/vpro.php
_internal/pc/wake.php
_internal/error_u201409.txt
_internal/runcmd.php
_internal/getConfiguration.php
ews/autoload.php
ews/del.php
ews/mod.php
ews/sync.php
utils/backup/backup_server.php
utils/backup/restore_server.php
MyScreens/timeline.config
kreator.html5/test.php
addedlogs.txt

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

Solution:

When processing a request, it should be checked whether the
requesting actor is authorized to access the resource.

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

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-2020-041

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-041.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:

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

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

iQIzBAEBCgAdFiEEZTiCFlVb++ceAX+9TH15zlMWMmgFAl/i+1MACgkQTH15zlMW
Mmh8TQ/+OOXO4wrTsludBFKgshYd7uhwxYv2S+FEZEglsHXjJ8yy92lxzvi9x8Yr
UmOGkILJMy0OPZKFUG+pMTpZ3+FVAvRPxK50GM2eC9F4cbRiz0N+N34ypL/r3UqO
iphpbbvlS67o7DfR8Jp0OcAAQ34vzbNE+LUDVvmyc/WxyCTk9SXOtrQflmK0Re9e
QRDcUmPNlkTyCfN4wV5VQHpJ+rhCnMg8LTle2k9EgTTyrWreqH2spG+xqr8vgWbe
5Tj07dQo9qE5oQDvkZcQGUkDi2+mmu6iFaHsVNOwtxHJbNJkfyG5ZYwURanjSuQn
gb8Qx6vx9EqHSxtEw7glSrtY2eJ/G/5XxQjR5T37Ouu9cAfcC4kk/+RJU4FgucU
2Zvkf/fXdCaYVElBQRpeZUo+gQ2xpC+/4DdIpoG7XI5iFg9YKaGcjqKNx4l5lbZl
zMkumuyrjdf5kf8bQm+fav3LKc58G6J8RUnh0r5RtLSpPNMwcfX5Bf1fs2G5p6VK
FRU5oI+TZOSeNgF/xLlbautyYNo4AqRGN9DlYo9PPsPSKsRxvV+3gwjxdCAHfyi7
YBGg0iGFosmNsHpb4hxwnn/h0l/zHSubIIakv7fJIYU+iZDDhcyVDVN098FUAkWv
RqZz0JLwpOWTxLeEk2Ub0d7nHb8tuYCQvk2Y4TdwP4plJanZ4bs=
=NhQE
-----END PGP SIGNATURE-----

Attachment: OpenPGP signature
Description: OpenPGP digital signature

_____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/

Current thread:

SYSS-2020-041 Urve - Missing Authorization (CWE-862) ***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