

Search ...

Add New

Follow us on Twitter

Subscribe to an RSS Feed

URVE Software Build 24.03.2020 Missing Authorization

Authored by [Erik Steltzner](#) | Site [sysss.de](#)

Posted Dec 26, 2020

URVE Software build version 24.03.2020 suffers from a missing authorization vulnerability.

tags | [exploit](#)

advisories | [CVE-2020-29551](#)

SHA-256 | [5b50fb6ac4e7f08d9e0044e8d698f81756c260f1010c2d75ae42018e91683f6b](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

-----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 (CVE-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_v001409.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-reszerwacjl-sal>
- [2] Product Website for URVE
<https://urve.co.uk>
- [3] SysS Security Advisory SYSS-2020-041

- <https://www.sysss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-041.txt>
[4] SysS Responsible Disclosure Policy
<https://www.sysss.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@sysss.de

Public Key:
https://www.sysss.de/fileadmin/dokumente/PGPKeys/Erik_Steltzner.asc
Key ID: 0x4C7979CE53163268
Key Fingerprint: 6538 8216 555B FB27 1E01 7FBD 4C79 79CE 5316 3268

E-Mail: christoph.ritter@sysss.de
Public Key:
https://www.sysss.de/fileadmin/dokumente/PGPKeys/Christoph_Ritter.asc
Key ID: 0x05458E66D35EAE8
Key Fingerprint: 9FB0 1B98 2F72 3D05 3AF3 62D8 0545 8E66 6D35 EAE8

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
nu11security 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	

File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)

Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)

Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

Systems

Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

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-----

iQI=BAEBCgAdFIEZT1CF1Vb++ceAX+9TH15z1M0MmgFAL/1+1MACgkQTH15z1M0M
Mmh8TQ/+0OX04wrTslud8FKgahYd7uhwxYv2S+FEZEg1sHXJJB8y921xzvi9x8Yr
UmOGkILJMy00PZKFUG+pmTtp23+PVAvrFpK50GM2ec9F4cbR1z0N+N34ypL/r30qQ
1phghabv1S67o7DFR83p00c3AQ34vz8NE+LIDVwmyc/WxyCTV9S30c+Q1m80a9e9e
QRDcUtmPN1kTyCFN4wV5VQHpJ+rhCnMg8LT1e2k9gTZYrWreqH2apG+xqr8vgWbe
5Tj07dQo9gE5oQDvk2cQGUKD12+mmu61FaHaVN0wtxHJbNJkfyG52YwURanJSuQn
gb8Qk6vx9Eg8SktEw7g1SrtV2eJ/G/5XxQJ85T370uu9CAfcC4kk/+RJU4FggucU
22vxf/fX8CAVVE1BQRpeEDcvgQ0xpc+/4DdIpoG7X13iPg9YKaGc-jgRkM4151bZ1
zMKumuyrjdf5kf8BQm+fav3LkC58G6J880nh0r58tLSpPNMwcfX5Bf1fa2G5p6VX
FRU5oI+TZ0SeNgF/xLLbavtYNo4AqRGN9D1Yo9PPaP8KaRwV+3gwJxdCAHfyI7
YB8g01GFosmN8Hpb4hxwnn/h01/zRSubIiakv7fJ1YU+1ZDDhcyVDVN098FUAKwV
Rqg20JLwpOWTxLeEk2Ub0d7nHb8tuYQvK2Y47dwP4p1Jan24bs=
~NhQR
-----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



© 2022 Packet Storm. All rights reserved.

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