ZKBio Time - CSV Injection

By Aamir Rehman - September 08, 2022

Hi all,

I am here with new post. Recently I have identified a csv injection vulnerability in one of the web-based time and attendance management software. Below are the details:

Software Description:

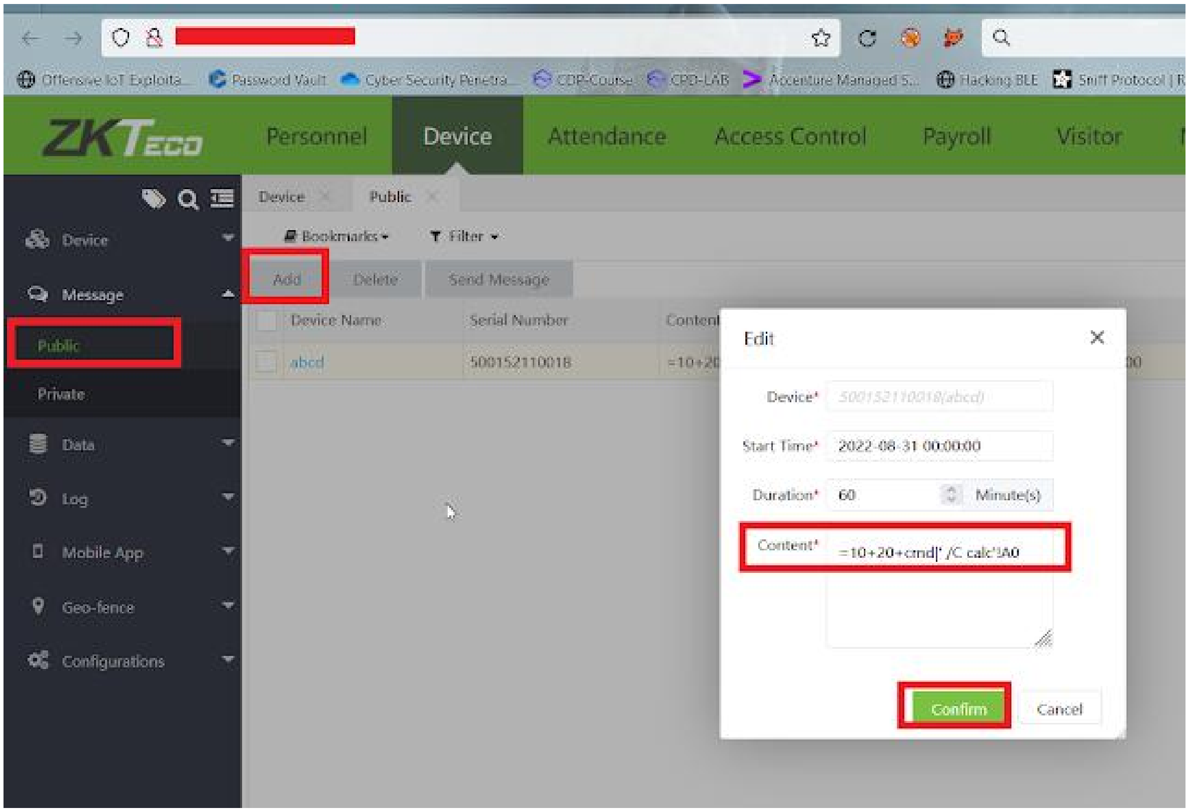
ZKBio Time is a powerful web-based time and attendance management software. With a powerful data handling capacity, the system can manage the attendance data of 10,000 employees. It can easily handle hundreds of devices and thousands of employees and their transactions. ZKBio Time comes with an intuitive user interface is able to manage timetable, shift and schedule and can easily generate attendance reports.

Impacted Version: 8.0.7 (Build: 20220721.14829) and before.

CVE ID: CVE-2022-40472

Vulnerability details:

1. Login to ZKBio Time Application
2. In the left Menu click on Messages -> Public
3. Click on ADD new message button
4. Write your Device Serial Number
5. Mention any date/time and duration
6. In Content Field Add your CSV injection payload.
7. As shown below



Device Name	Serial Number	Content
abcd	500152110018	=10+20

Edit

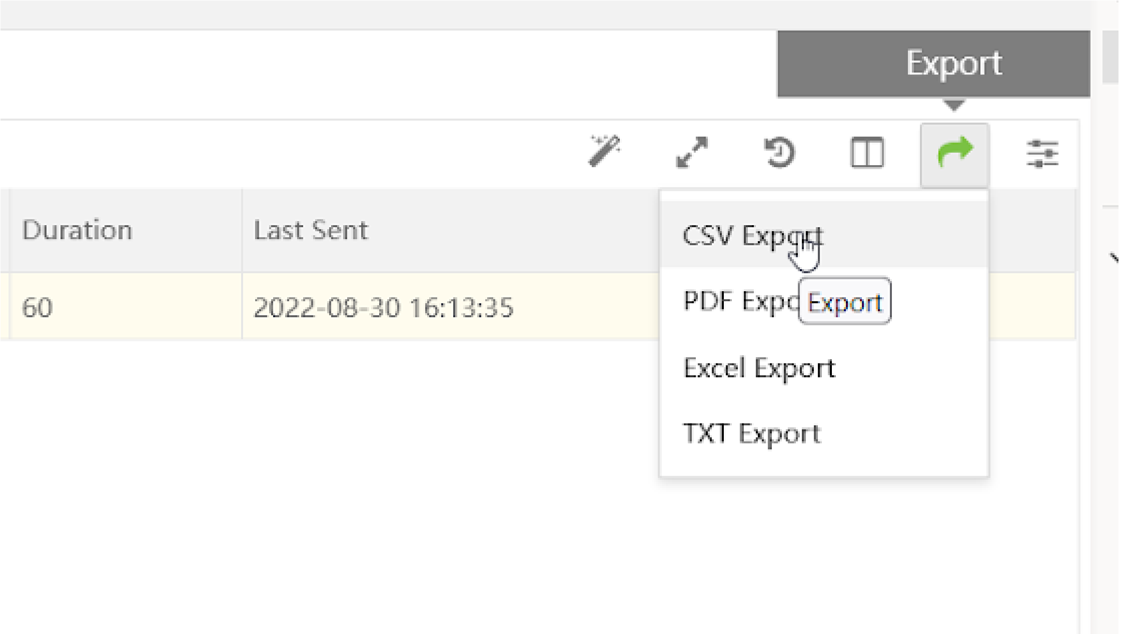
Device* 500152110018(abcd)

Start Time* 2022-08-31 00:00:00

Duration* 60 Minute(s)

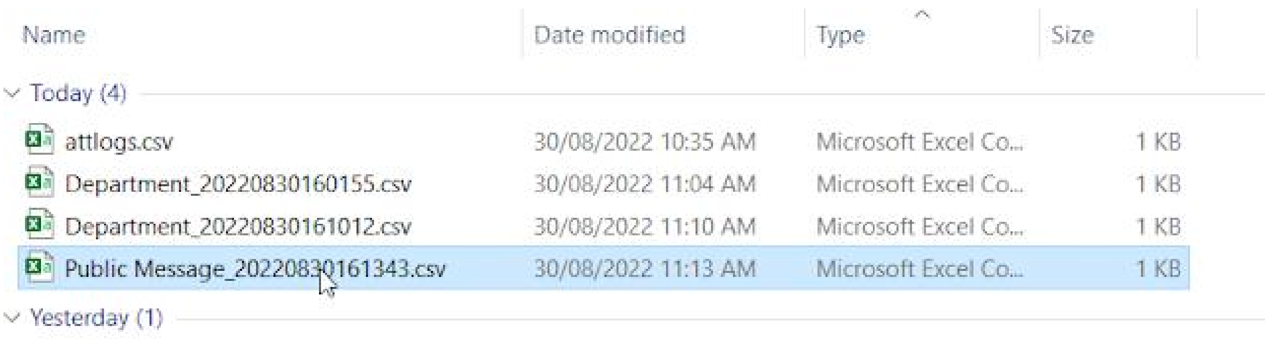
Content* =10+20+cmd|' /C calc'!A0

8. Any user who extract the report in CSV format and opens it
9.



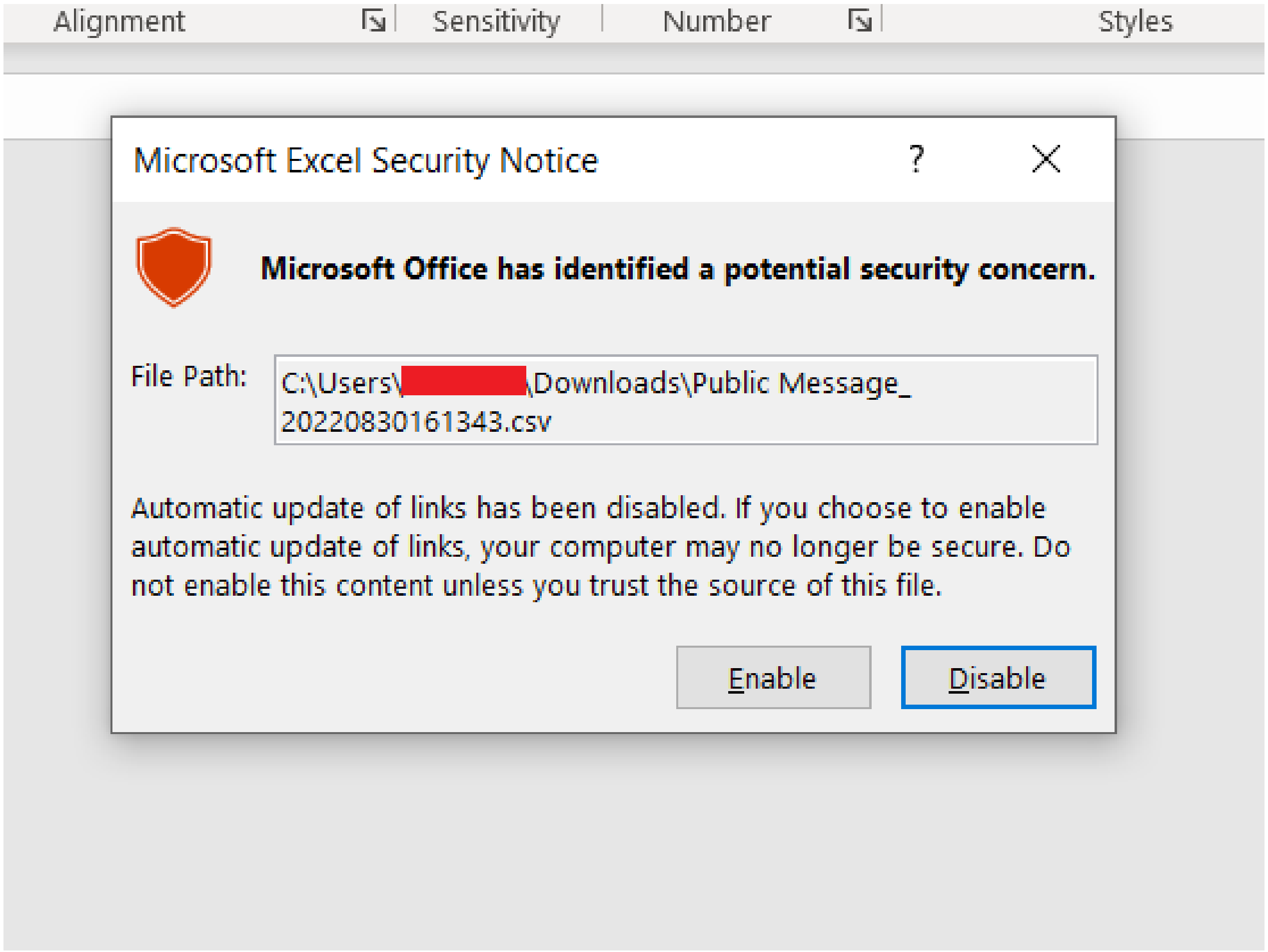
Duration	Last Sent
60	2022-08-30 16:13:35

10. The embedded payload will be executed



Name	Date modified	Type	Size
Today (4)			
attlogs.csv	30/08/2022 10:35 AM	Microsoft Excel Co...	1 KB
Department_20220830160155.csv	30/08/2022 11:04 AM	Microsoft Excel Co...	1 KB
Department_20220830161012.csv	30/08/2022 11:10 AM	Microsoft Excel Co...	1 KB
Public Message_20220830161343.csv	30/08/2022 11:13 AM	Microsoft Excel Co...	1 KB
Yesterday (1)			

There is 90% chance that user will ignore the below warning box as the report is downloaded from trusted source. This will lead to payload execution.



Microsoft Excel Security Notice

Microsoft Office has identified a potential security concern.

File Path: C:\Users\[redacted]\Downloads\Public Message_20220830161343.csv

Automatic update of links has been disabled. If you choose to enable automatic update of links, your computer may no longer be secure. Do not enable this content unless you trust the source of this file.

Thanks

To leave a comment, click the button below to sign in with Google.

SIGN IN WITH GOOGLE

Popular posts from this blog

Ericsson BSCS iX R18 Billing & Rating (ADMX, MX) - Stored XSS

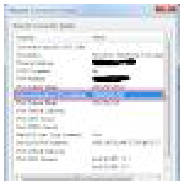
By Aamir Rehman - January 30, 2020

Dear Reader, I was able to identify stored XSS in multiple web base modules of Ericsson BSCS iX R18 Billing & Rating platform Below are its details: # Software description: Ericsson Billing is a convergent billing so …

READ MORE

Autoconfiguration ipv4 address 196.254.x.x IP Problem

By Aamir Rehman - April 12, 2013



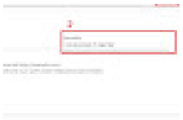
Today when i connect my laptop to Lan it wasn't getting the ip from my DHCP server. Instead it gives me some weird IP like 196.254.x.x . while my Wifi was working fine, I searched Alot to get to know until i four …

READ MORE

CSV Injection in Acunetix version 13.0.201217092

By Aamir Rehman - April 11, 2022

Hi all, I was using Acunetix version 13.0.201217092 for scanning purposes



back in Jan 2021, and I was able to identify CSV Injection vulnerability in the web scanner. Any user who is not the administrator can perfor …

READ MORE

Contributors

AAMIR REHMAN

ASAD ULLAH

Subscribe Us via email

Enter your email address:

Subscribe

Archive

GHDB For any Website

example.com

Type in your domain & Click Below Links

- APIs Leak via Postman
- Publicly exposed documents
- Directory listing vulnerabilities
- Configuration files exposed
- Database files exposed
- Log files exposed
- Backup and old files
- Login pages
- SQL errors
- PHP errors/warnings
- phpinfo()
- Search Pastebin.com
- Search Github/Gitlab
- Search Stackoverflow
- Signup pages