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 perform these actions which can lead to admin system compromise. For testing I used the Admin account.

Lets get to the technical details.

CVE ID Assigned: CVE-2022-29315

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29315

https://www.cve.org/CVERecord?id=CVE-2022-29315

Vulnerable Version: Before version 14

Fixed Version: 14 and 14+

# Software description:

Acunetix by Invicti Security is an application security testing tool built to help small & mid-size organizations around the world take control of their web security.

# Technical Details & Impact:

It was observed that **Target** page is vulnerable to CSV Injection, using CSV injection; Maliciously crafted formulas can be used for three key attacks:

Hijacking the user's computer by exploiting vulnerabilities in the spreadsheet software, such as CVE-2014-3524.

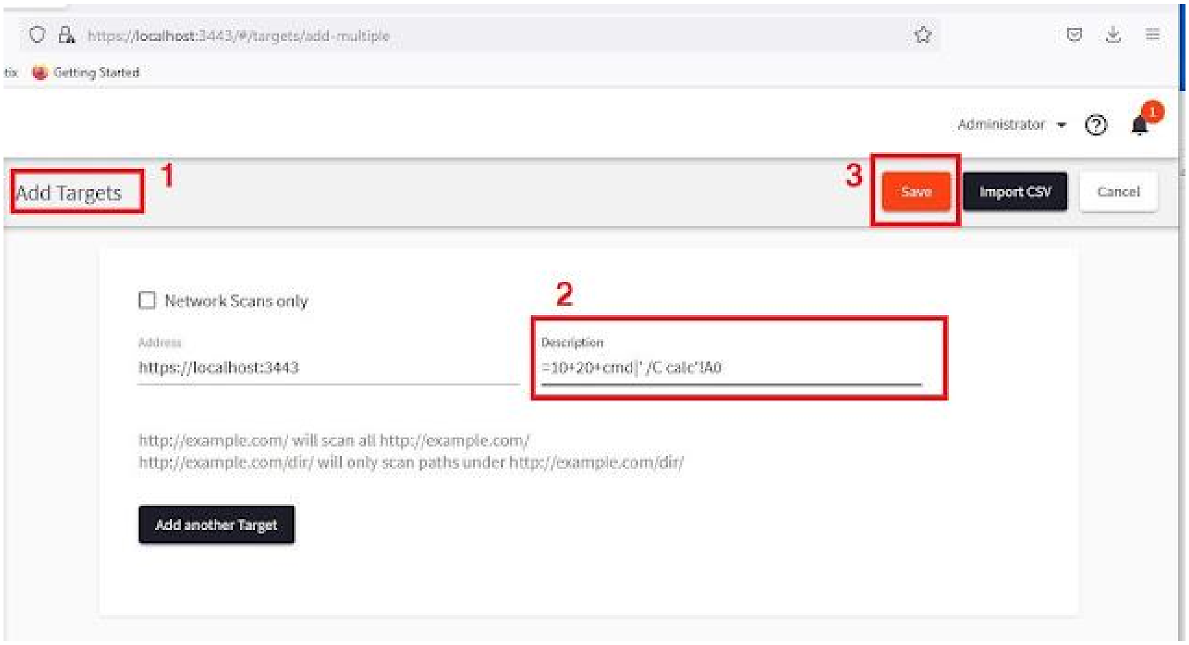
Hijacking the user's computer by exploiting the user's tendency to ignore security warnings in spreadsheets that they downloaded from their own website.

Exfiltrating contents from the spreadsheet, or other open spreadsheets.

# POC

To start the scan in Acunetix version 13.0.201217092 you have to add the target.

1. Click on "Add Target"
2. Add any target address and in description add CSV Injection Payloads for test I have used **"=10+20+cmd|' /C calc'!A0"**
3.

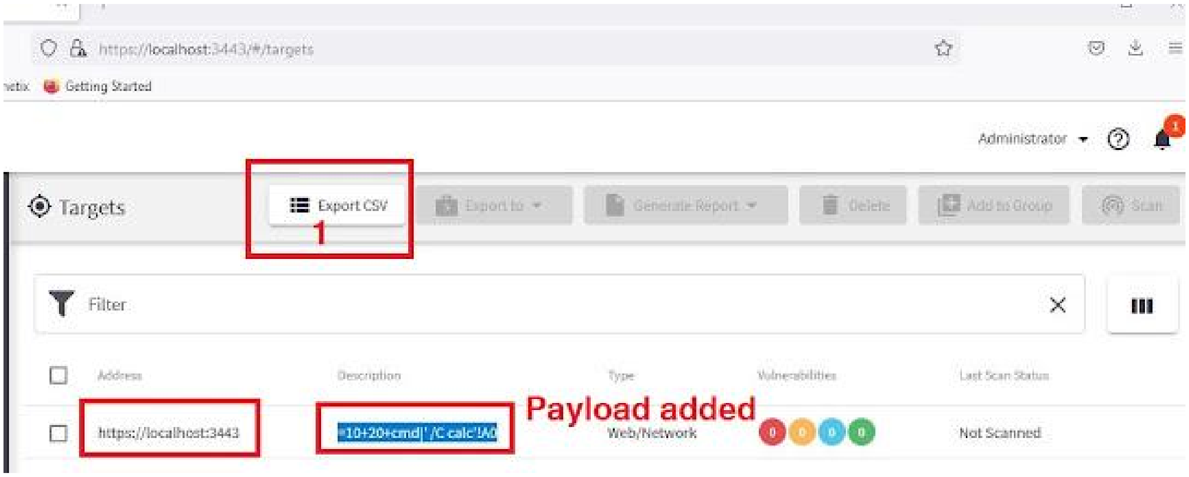


Address: https://localhost:3443

Description: =10+20+cmd|' /C calc'!A0

http://example.com/ will scan all http://example.com/
http://example.com/dir/ will only scan paths under http://example.com/dir/

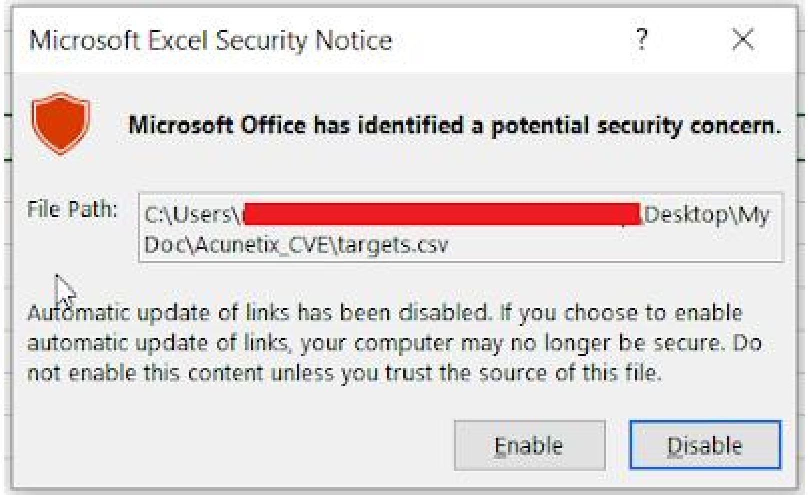
4. Click on **Save** button
5. The target with malicious payload will be shown in description column.
6. Click on **Export CSV** button
7.



Address	Description	Type	Vulnerabilities	Last Scan Status
https://localhost:3443	=10+20+cmd|' /C calc'!A0	Web/Network	0 0 0 0	Not Scanned

8. CSV will be download and upon opening it will ask for Enable execution
9. Click on enable as the Admin will alwavs trust the downloaded since it downloaded from

trusted source, Once enabled it will execute the payload


Microsoft Excel Security Notice

Microsoft Office has identified a potential security concern.

File Path: C:\Users\[redacted]Desktop\My Doc\Acunetix_CVE\targets.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.

Vulnerability was reported to Acunetix they silently fixed in latest version after 13.0. I have verified its fixed on 14.7.22xxxx

Thanks

Acunetix csv injection | Acunetix-CVE | Acunetix-exploit | Acunetix-vulnerability

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

SIGN IN WITH GOOGLE

Popular posts from this blog

Popular posts from this blog

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

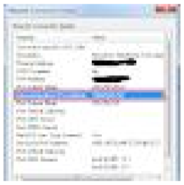
By Aamir Rehman - January 30, 2020

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

Powered by Blogger

Theme images by Michael Elkan

←

Contributors

AAMIR REHMAN

ASAD ULLAH

Subscribe Us via email

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