

Developers Blog

This is a personal blog for two users, here we share all the problems which we face in our daily life during penetration testing activities or during other software development activities. Further you can ask us any question regarding our posts in comments.

NetSkope Unauthenticated CSV Injection in Admin UI



By [Aamir Rehman](#) - November 12, 2020

This post is related to CSV injection in netskope Admin UI (Version 75.0) where an unauthenticated user can inject malicious payload in audit logs of admin portal and once the admin extract and open the report, the malicious payload will be executed.

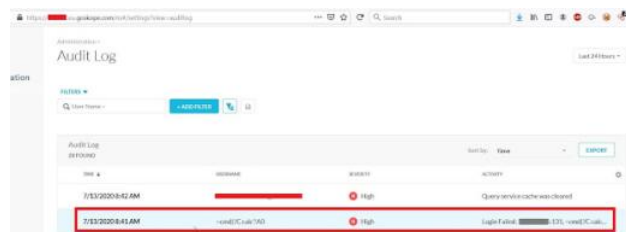
Test case: The audit logs consist of login attempts which includes username, for test case I have injected a non-malicious payload in username field, this payload was reflecting in audit logs and was executed once we download and open the report.

Exploitation:

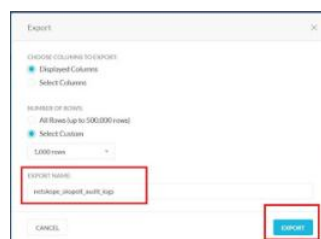
In below screenshot you can see a sample csv injection payload and a dummy password.



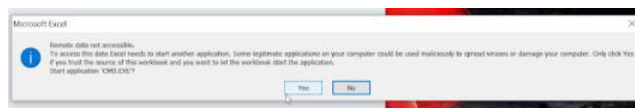
To verify if our payload is reflecting in Audit logs of admin portal, we logged-in as an admin and in below screenshot our payload can be seen

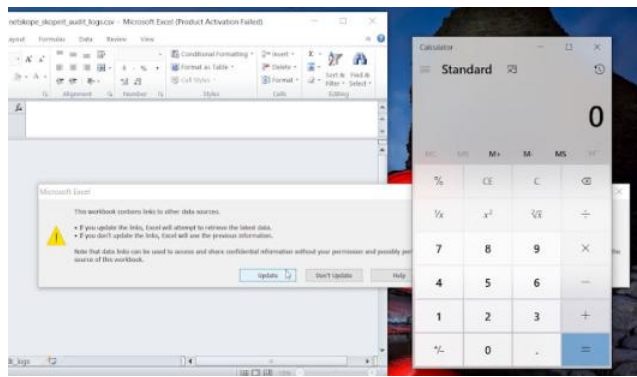


Admin of Netskope admin extracted and downloaded the report.



Admin opens the downloaded reported and our payload got executed.





This Vulnerability has been fixed now in the latest version of NetSkope and CVE ID : CVE-2020-28845 has been assigned by Mitre Team.

Big thanks to Deepak Venkataravanappa from netskope team for his communications throughout this remediation cycle.

Thanks.

Aamir Rehman Yousafzai.

 [csv injection](#) [CVE](#) [CVE-2020-28845](#) [netskope](#) [netskope cve](#) [netskope vulnerability](#)

To leave a comment, click the button below to 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 solution for telecoms that combines an unrivaled combination of out-of-the-box fea ...

[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 found a great piece of code on a blog. so going to share with you guys. Problem with my lq ...

[READ MORE](#)

ZKT Eco ADMS - Stored XSS

By Aamir Rehman - September 27, 2022



Hi All, I was able to identify stored XSS in one online attendance system i.e. ZKT Eco ADMS (v 3.1-164) (Automatic Data Master Server) is a powerful web-based time and attendance management software. which is used to configure the attendance devices and manage its users. Cve ID assigned ...

[READ MORE](#)

 Powered by Blogger

Theme images by Michael Elkan



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