

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.

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



By [Amir 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 features and high configurability.

As an evolution of the widely-installed Ericsson BSCS iX, Ericsson Billing provides a low-risk but effective route to capture and secure revenue streams and take advantage of business opportunities from both traditional telecom services as well as digital services, 5G and IoT.

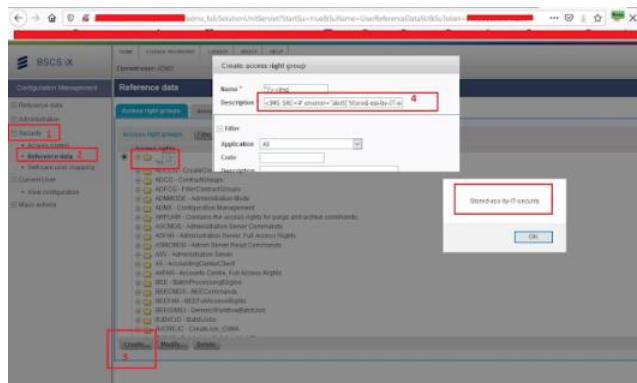
Technical Details & Impact:

There are multiple web base modules in BSCS iX e.g. ADMX, MX (monitoring center), CX etc. It was observed that ADMX and MX are vulnerable to stored XSS, In most test cases session hijacking was also possible by utilizing the XSS vulnerability. This potentially allows for full account takeover, or exploiting admin's browsers using beef framework

POC

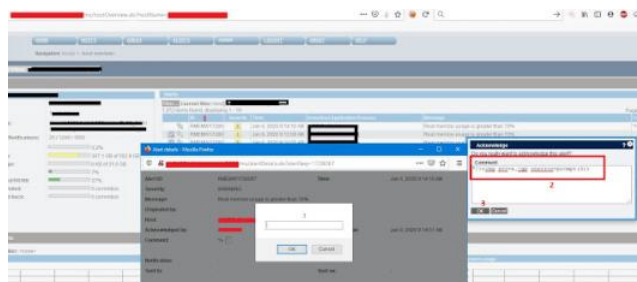
ADMX:

1. Once user logged-in on portal visit "/ADMX/solutionUnitServlet?SuName=UserReferenceDataSU" it will open Reference Data. If it shows error you can manually visit the page by clicking the "Security Tab", click on "Reference Data Tab".
2. Create a new "Access Rights Group", enter anything as name and in description enter your xss payload.
3. Click Save and your Stored XSS will be executed.



MX:

1. MX Portal is used for monitoring the health/storage of all machines or scheduling any task using this portal.
2. The "Alert Dashboard" section is vulnerable to stored xss.
3. Double click on any alert on dashboard and in comment section enter your xss payload, click OK and you xss will stored permanently, and even admins/super admin cannot remove the xss.



Update:

Two CVE IDs are assigned to these both findings.

CVE-2020-29144

CVE-2020-29145

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-29144>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-29145>

Thanks



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



Popular posts from this blog

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:

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](#)