9thplayer / gist:df042fe48c314dbc1afad80ffed8387d

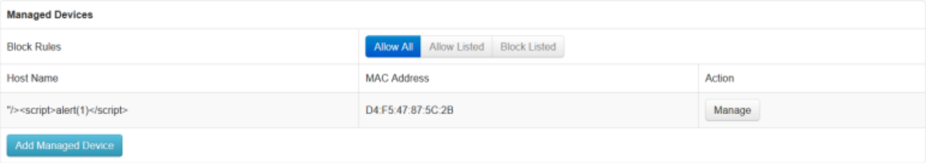
Created 2 years ago

Hitron Router - CODA - 4582U - 7.1.1.30 - Stored XSS Vulnerability

gistfile1.txt

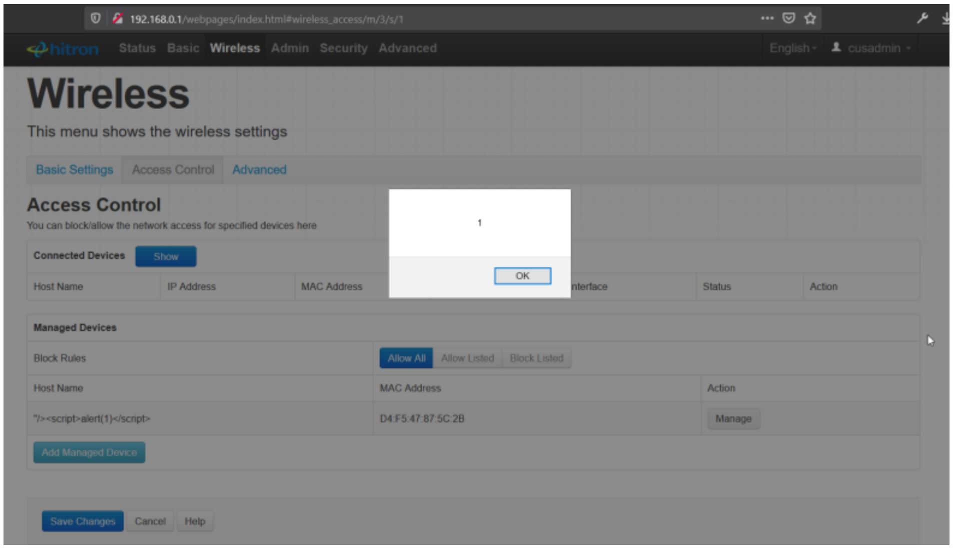
```
Hitron CODA-4582U 7.1.1.30 devices allow XSS via a Managed Device name on the > Wireless > Access Control > Add Managed Device screen.

Impact:
Script can be stored in Database and execute every time when users visits it. If an attacker can control a script that is executed in the v
Amongst other things, the attacker can:
1) Perform any action within the application that the user can perform.
2) View any information that the user is able to view.
3) Modify any information that the user is able to modify.
4) Initiate interactions with other application users, including malicious attacks, that will appear to originate from  the initial victim

Attack Vector:
To exploit this vulnerability user must visit the Add managed device and click on manage and it will trigger XSS payload.

POC:

When user adds the Managed Device to the Wireless - Access Control - Add Managed Device list, It asks for Device name and MAC address.
In-place of device's name, need to add XSS payload and click on Apply.

Payload is "/><script>&#97;lert(document.cookie)</script>
initially payload may not work so use payload <svg><script>&#97;lert(1)</script></svg> and remove svg tags and add "/> before the payload a
and when you click on manage, it will trigger payload.
```

9thplayer commented on Feb 18, 2020 Author



Managed Devices

Block Rules	Allow All / Allow Listed / Block Listed	
Host Name	MAC Address	Action
"/><script>alert(1)</script>	D4:F5:47:87:5C:2B	Manage



192.168.0.1/webpages/index.html#wireless_access/m/3/s/1

Wireless

This menu shows the wireless settings

Access Control

You can block/allow the network access for specified devices here

Connected Devices Show

Host Name	IP Address	MAC Address	nterface	Status	Action

1

Managed Devices

Block Rules	Allow All / Allow Listed / Block Listed	
Host Name	MAC Address	Action
"/><script>alert(1)</script>	D4:F5:47:87:5C:2B	Manage