NVS Security

Network scanner

Contents

Introduction.

Controlling your own networks is an important part of countering potential attacks from hackers. Knowing the status of open ports, vulnerabilities, and managing the installation of updates based on real threats allows you to prevent most attempts to invade the infrastructure and react to an attack in time.
NVS uses free software included in the Kali Linux operating system:

-nmap

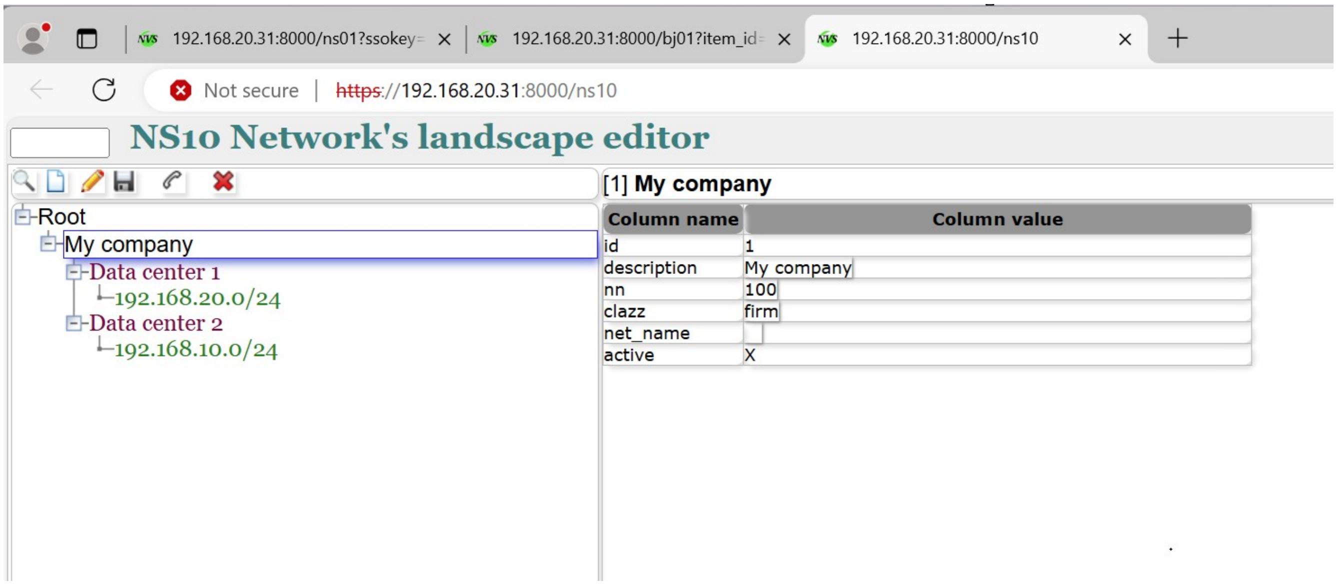
-metasploit

, etc.
by analyzing and processing the results, informing users about the problems found.
NVS also includes a report that serves as an anti-scanner that warns administrators
if it suspects scanning the ports of the monitor itself.

Note: to use NVS Security feature it is mandatory to install NVS system on Kali Linux operation system. More details you can find in guide “Installation NVS on Kali”.

Describe your network landscape

Use tcode **Ns10 Network editor** to describe your network list in hierarchy.


192.168.20.31:8000/ns01?ssokey=
192.168.20.31:8000/bj01?item_id=
192.168.20.31:8000/ns10
Not secure
~~https~~://192.168.20.31:8000/ns10

NS10 Network's landscape editor

```
Root
  My company
    Data center 1
      192.168.20.0/24
    Data center 2
      192.168.10.0/24
```

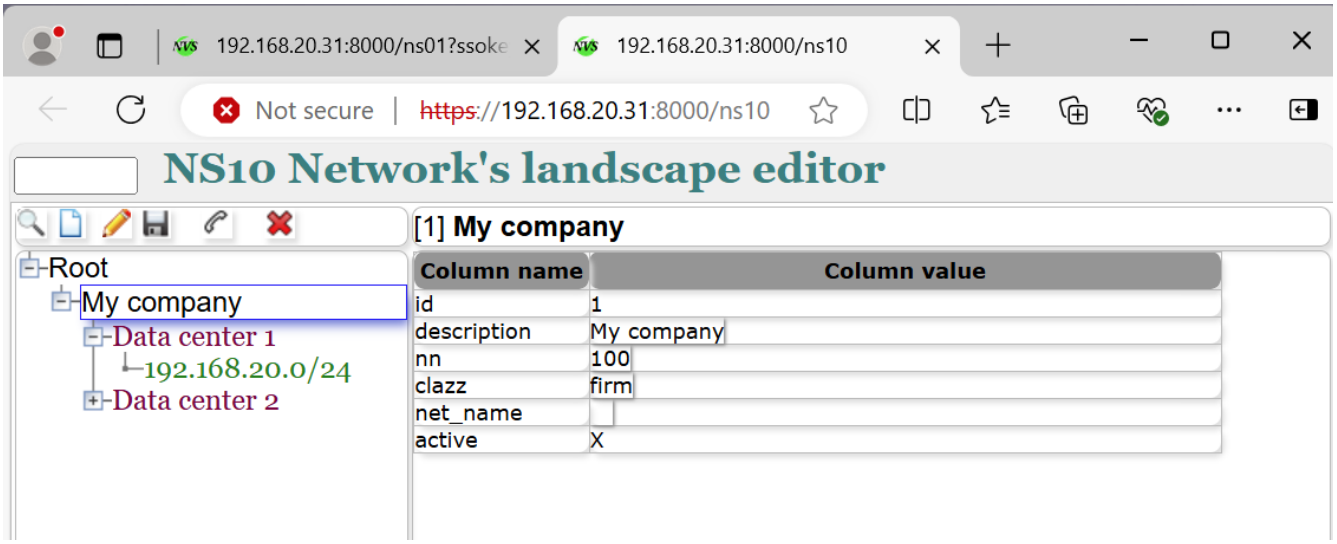
[1] **My company**

Column name	Column value
id	1
description	My company
nn	100
clazz	firm
net_name	
active	X

To decorate text in the tree, change column “clazz”. You can set

- firm
- location
- network

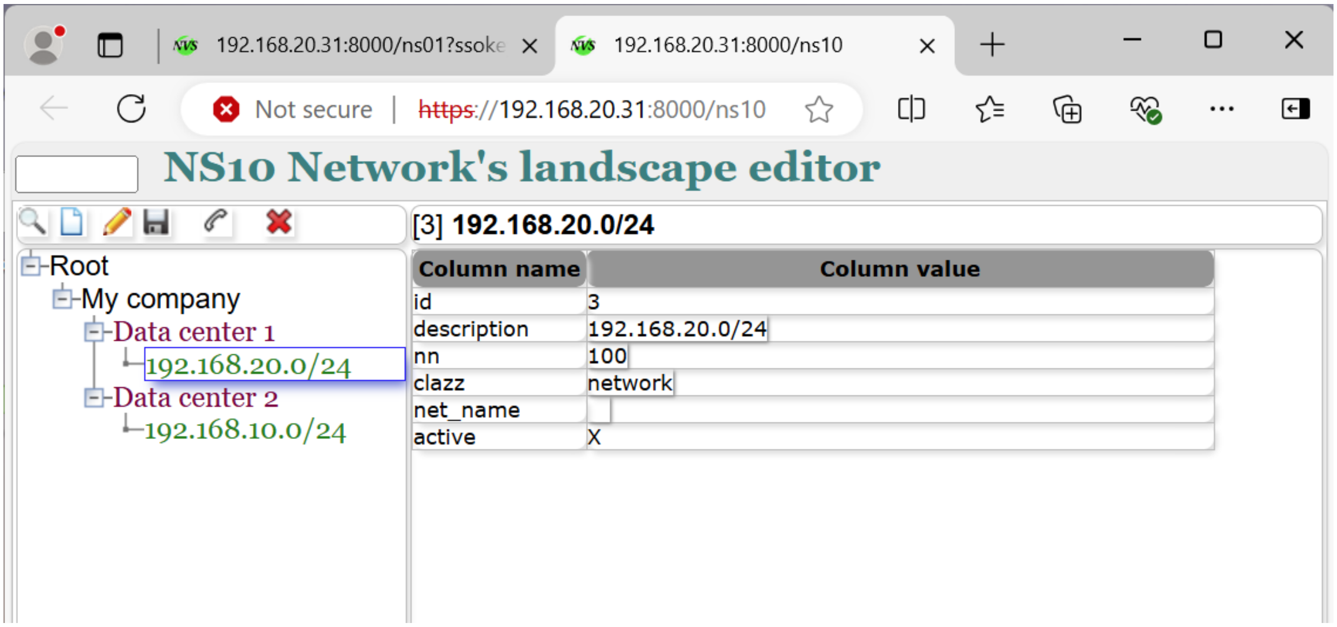
“firm” for company, “location” for 2-th level (Datacenter, Building,and etc.) and “network”.


192.168.20.31:8000/ns01?ssoke
192.168.20.31:8000/ns10
Not secure
https://192.168.20.31:8000/ns10
NS10 Network's landscape editor
Root
My company
Data center 1
192.168.20.0/24
Data center 2

[1] My company

Column name	Column value
id	1
description	My company
nn	100
clazz	firm
net_name	
active	X

Finally, you will see something like this:


192.168.20.31:8000/ns01?ssoke
192.168.20.31:8000/ns10
Not secure
https://192.168.20.31:8000/ns10

NS10 Network's landscape editor

Root
My company
Data center 1
192.168.20.0/24
Data center 2
192.168.10.0/24

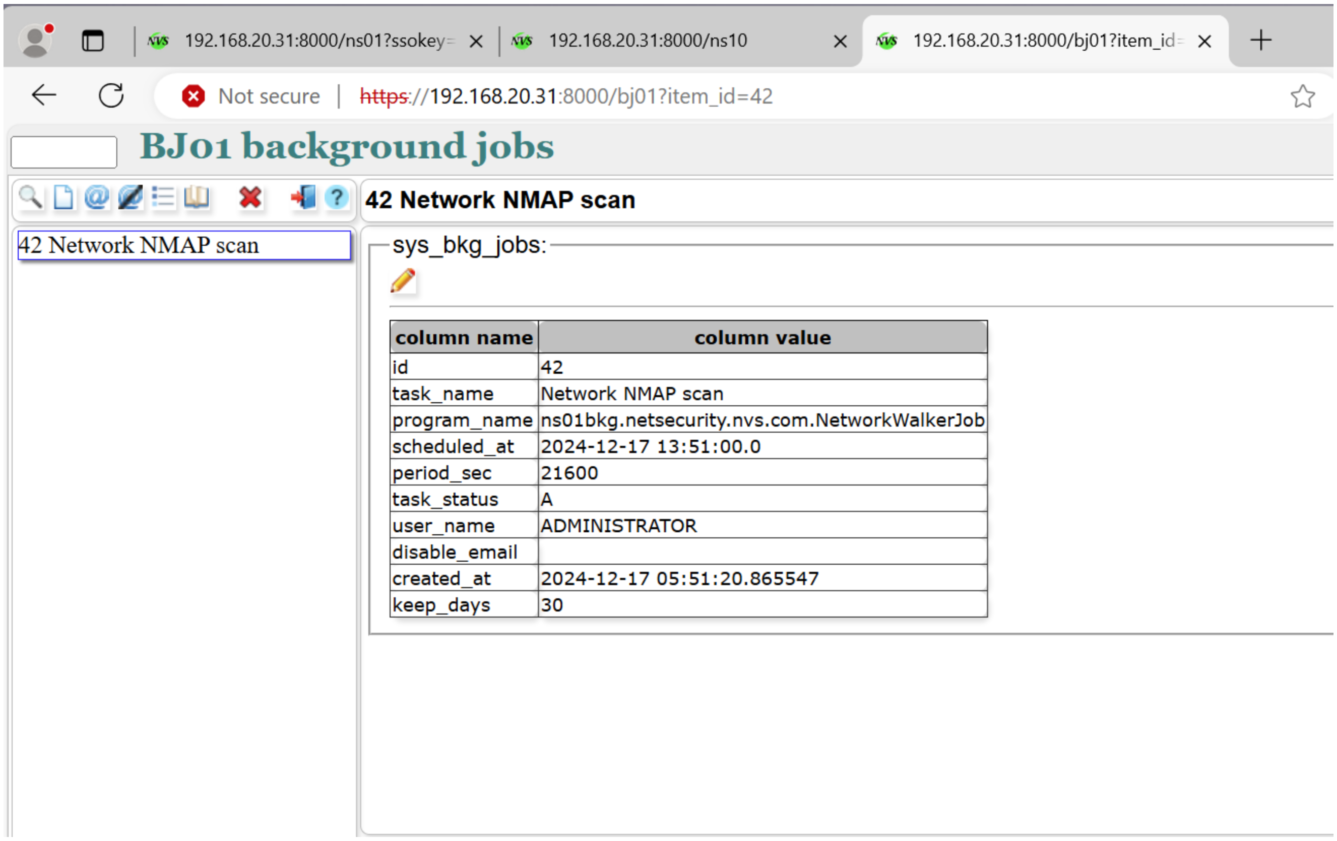
[3] **192.168.20.0/24**

Column name	Column value
id	3
description	192.168.20.0/24
nn	100
clazz	network
net_name	
active	X

Schedule background job for network scan

In tcode Bj01 schedule background job to collect data on regular basis. Remember that scan of networks is time-consuming process and it is good idea do not start it too often.

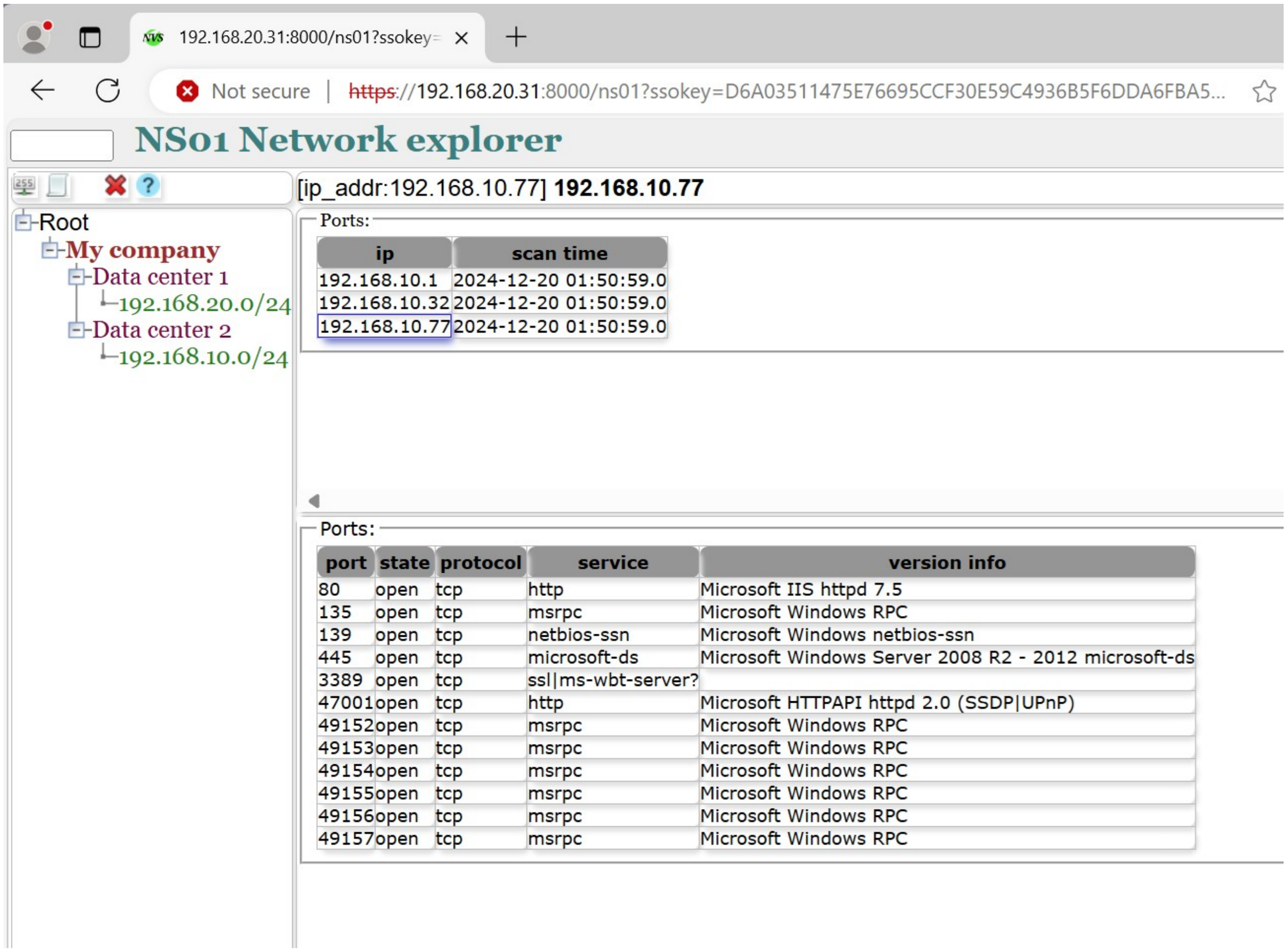
Search job name by key “netsecurity” for example.



column name	column value
id	42
task_name	Network NMAP scan
program_name	ns01bkg.netsecurity.nvs.com.NetworkWalkerJob
scheduled_at	2024-12-17 13:51:00.0
period_sec	21600
task_status	A
user_name	ADMINISTRATOR
disable_email	
created_at	2024-12-17 05:51:20.865547
keep_days	30

Check your IP’s and open ports

After scan is finished, you can check all found active devices and open ports. All scan results are saved in tables of NVS database and history is available



192.168.20.31:8000/ns01?ssokey=
Not secure
~~https~~://192.168.20.31:8000/ns01?ssokey=D6A03511475E76695CCF30E59C4936B5F6DDA6FBA5...
NS01 Network explorer
Root
My company
Data center 1
192.168.20.0/24
Data center 2
192.168.10.0/24

[ip_addr:192.168.10.77] **192.168.10.77**

Ports:

ip	scan time
192.168.10.1	2024-12-20 01:50:59.0
192.168.10.32	2024-12-20 01:50:59.0
192.168.10.77	2024-12-20 01:50:59.0

Ports:

port	state	protocol	service	version info
80	open	tcp	http	Microsoft IIS httpd 7.5
135	open	tcp	msrpc	Microsoft Windows RPC
139	open	tcp	netbios-ssn	Microsoft Windows netbios-ssn
445	open	tcp	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389	open	tcp	ssl|ms-wbt-server?	
47001	open	tcp	http	Microsoft HTTPAPI httpd 2.0 (SSDP|UPnP)
49152	open	tcp	msrpc	Microsoft Windows RPC
49153	open	tcp	msrpc	Microsoft Windows RPC
49154	open	tcp	msrpc	Microsoft Windows RPC
49155	open	tcp	msrpc	Microsoft Windows RPC
49156	open	tcp	msrpc	Microsoft Windows RPC
49157	open	tcp	msrpc	Microsoft Windows RPC

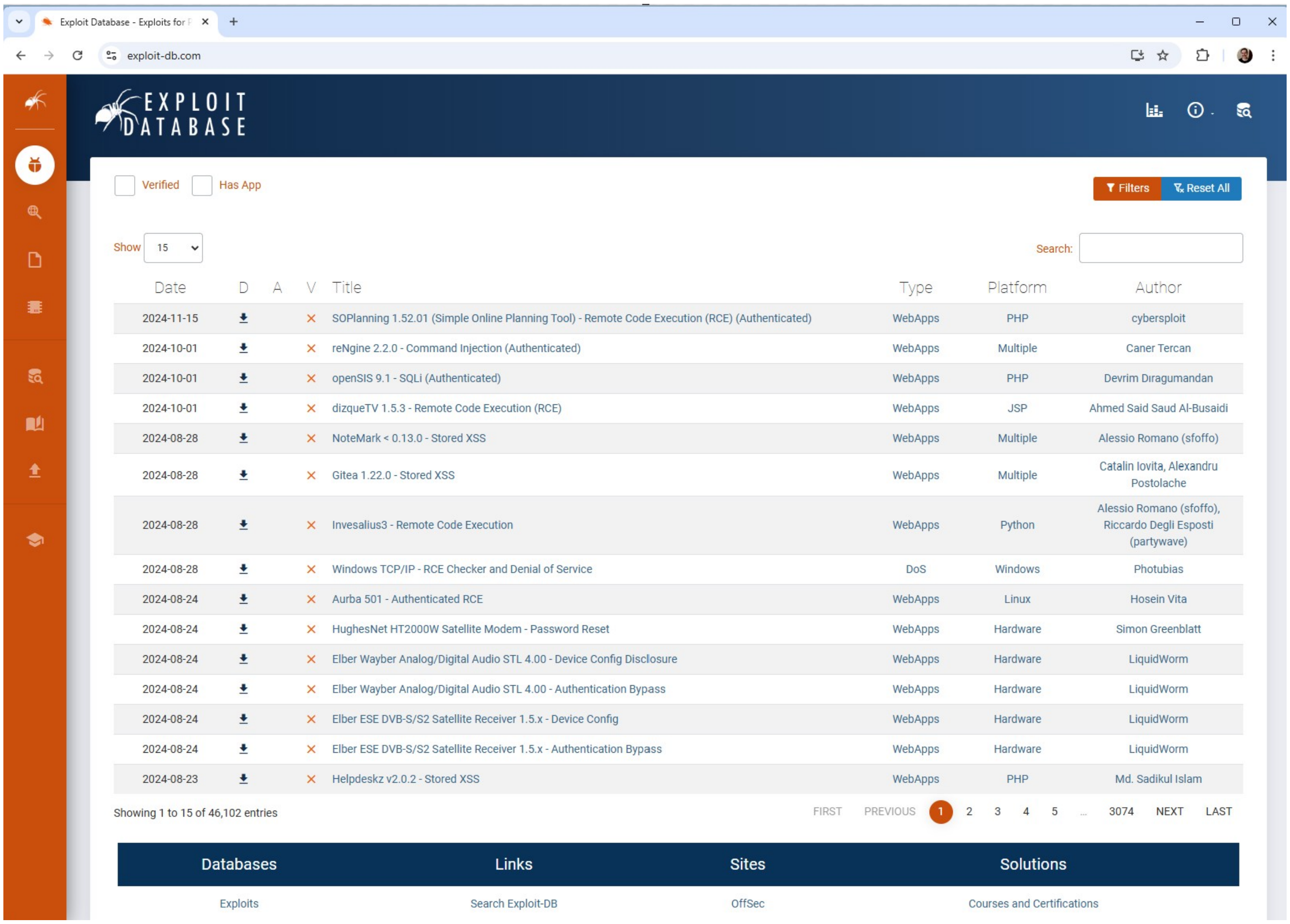
Vulnerability scanning

To scan for vulnerabilities, NVS uses the built-in Kali Linux tools , which in turn use publicly available databases in Internet.

https://www.exploit-db.com/

https://nvd.nist.gov/

https://vulners.com/



Date	D	A	V	Title	Type	Platform	Author
2024-11-15	⬇		✕	SOPlanning 1.52.01 (Simple Online Planning Tool) - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	cybersploit
2024-10-01	⬇		✕	reNgine 2.2.0 - Command Injection (Authenticated)	WebApps	Multiple	Caner Tercan
2024-10-01	⬇		✕	openSIS 9.1 - SQLi (Authenticated)	WebApps	PHP	Devrim Dragumandan
2024-10-01	⬇		✕	dizqueTV 1.5.3 - Remote Code Execution (RCE)	WebApps	JSP	Ahmed Said Saud Al-Busaidi
2024-08-28	⬇		✕	NoteMark < 0.13.0 - Stored XSS	WebApps	Multiple	Alessio Romano (sfoffo)
2024-08-28	⬇		✕	Gitea 1.22.0 - Stored XSS	WebApps	Multiple	Catalin Iovita, Alexandru Postolache
2024-08-28	⬇		✕	Invesalius3 - Remote Code Execution	WebApps	Python	Alessio Romano (sfoffo), Riccardo Degli Esposti (partywave)
2024-08-28	⬇		✕	Windows TCP/IP - RCE Checker and Denial of Service	DoS	Windows	Photubias
2024-08-24	⬇		✕	Aurba 501 - Authenticated RCE	WebApps	Linux	Hosein Vita
2024-08-24	⬇		✕	HughesNet HT2000W Satellite Modem - Password Reset	WebApps	Hardware	Simon Greenblatt
2024-08-24	⬇		✕	Elber Wayber Analog/Digital Audio STL 4.00 - Device Config Disclosure	WebApps	Hardware	LiquidWorm
2024-08-24	⬇		✕	Elber Wayber Analog/Digital Audio STL 4.00 - Authentication Bypass	WebApps	Hardware	LiquidWorm
2024-08-24	⬇		✕	Elber ESE DVB-S/S2 Satellite Receiver 1.5.x - Device Config	WebApps	Hardware	LiquidWorm
2024-08-24	⬇		✕	Elber ESE DVB-S/S2 Satellite Receiver 1.5.x - Authentication Bypass	WebApps	Hardware	LiquidWorm
2024-08-23	⬇		✕	Helpdeskz v2.0.2 - Stored XSS	WebApps	PHP	Md. Sadikul Islam

Showing 1 to 15 of 46,102 entries

Databases	Links	Sites	Solutions
Exploits	Search Exploit-DB	OffSec	Courses and Certifications

Conclusion

NVS Security is constantly evolving and to keep up to date with all available scanning tools , please visit the website www.nvs-itech.com

Thank you!