FortiGate Firewall Configs Dumped: Revisiting CVE-2022-40684 Exploitation

socradar.io/fortigate-firewall-configs-cve-2022-40684-exploitation/

January 16, 2025

Home
Resources

Blog

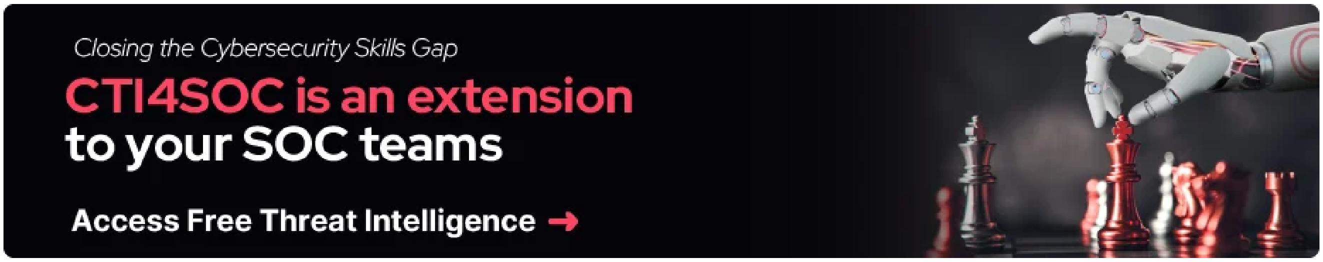
Jan 16, 2025

7 Mins Read

[Update] January 18, 2025: “Fortinet’s Official Statement on the Breach”

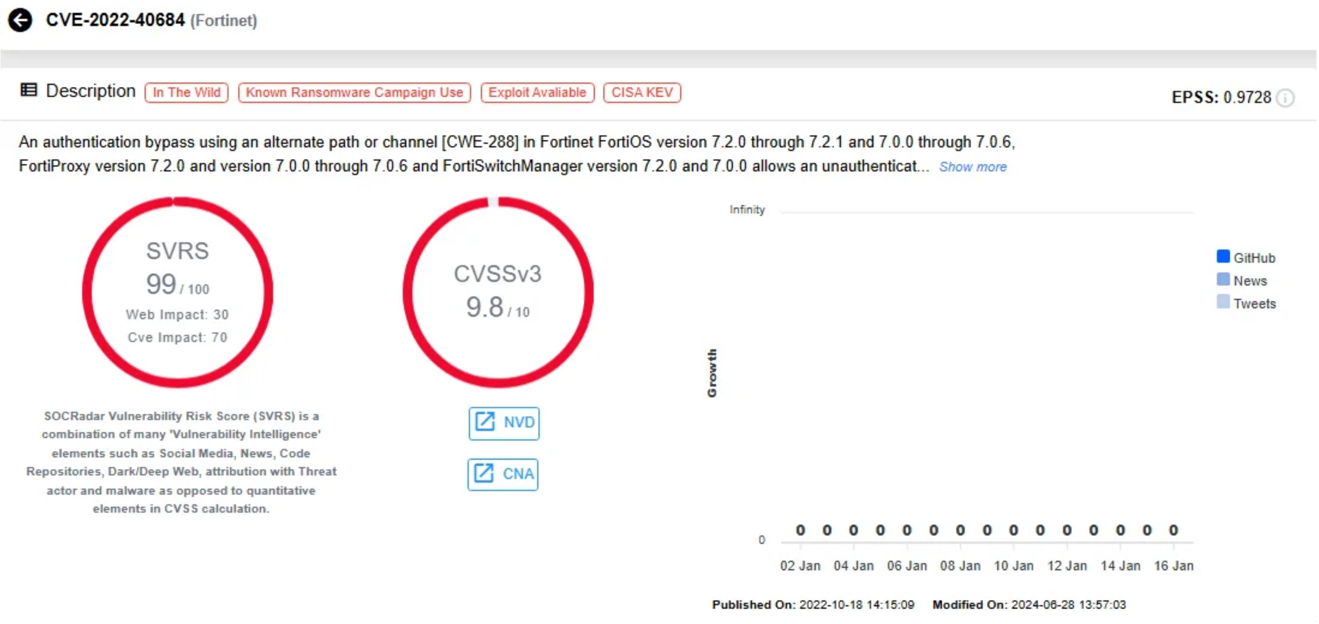
In a shocking development, the fallout from the 2022 Fortinet vulnerability, CVE-2022-40684, has resurfaced with severe consequences. A newly emerged group, Belsen Group, has released configurations from over 1**5,000 compromised FortiGate firewalls**.

This breach not only exposes usernames, passwords (some in plaintext), and VPN credentials but also includes critical firewall rules, IP addresses, and digital certificates, underscoring the lingering impact of vulnerabilities even years after patching.


Closing the Cybersecurity Skills Gap
CTI4SOC is an extension
to your SOC teams
Access Free Threat Intelligence →

The Exploit: A Critical Authentication Bypass

Originally discovered in 2022, CVE-2022-40684 was a severe **authentication bypass vulnerability** with a **CVSS score of 9.8**. Exploited actively in the wild, it allowed remote attackers to gain administrative access to Fortinet devices via specially crafted HTTP or HTTPS requests. Vulnerable versions included FortiOS (7.0.0–7.0.6 and 7.2.0–7.2.1), FortiProxy (7.0.0–7.0.6 and 7.2.0), and FortiSwitchManager (7.0.0 and 7.2.0).



CVE-2022-40684 (Fortinet)

Description In The Wild | Known Ransomware Campaign Use | Exploit Avaliable | CISA KEV

EPSS: 0.9728

An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticat... Show more

SVRS 99 / 100
Web Impact: 30
Cve Impact: 70

SOCRadar Vulnerability Risk Score (SVRS) is a combination of many 'Vulnerability Intelligence' elements such as Social Media, News, Code Repositories, Dark/Deep Web, attribution with Threat actor and malware as opposed to quantitative elements in CVSS calculation.

CVSSv3 9.8 / 10

Published On: 2022-10-18 14:15:09 Modified On: 2024-06-28 13:57:03

Vulnerability card of CVE-2022-40684 (SOCRadar Vulnerability Intelligence)

Though patches were promptly issued by Fortinet, reports emerged of attackers exploiting unpatched systems, leading to unauthorized access to sensitive configurations. GreyNoise and Shodan searches during the exploit's peak highlighted **over 165,000 publicly exposed FortiGate firewalls**, indicating the scope of the threat.

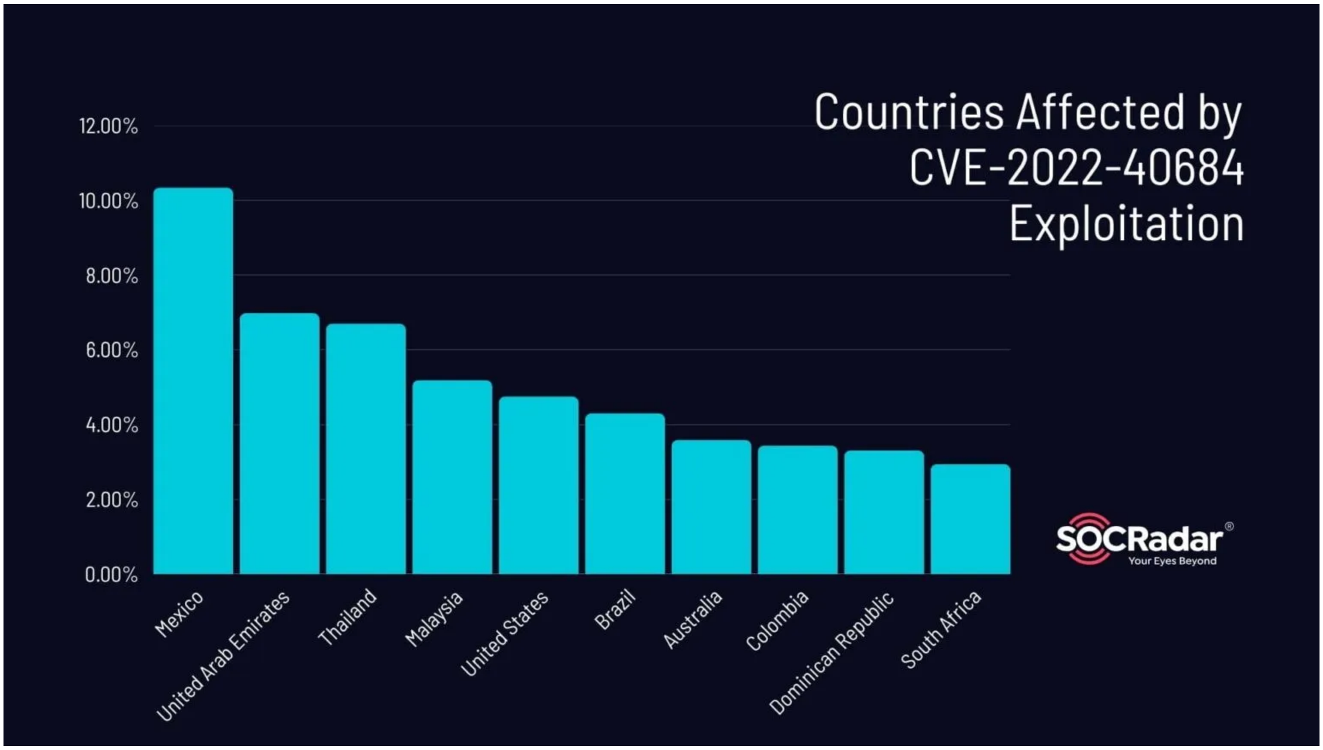
The Fallout: 2022 Exploits Surface in 2025

The Belsen Group's recent release of compromised firewall configurations reveals that many organizations were exploited before patching their systems. The leaked data includes detailed configurations and plaintext VPN credentials, posing significant risks:

- **Network security compromised:** Attackers now have access to detailed firewall rules, potentially enabling them to evade defenses.
- **Credential exposure:** Plaintext usernames and passwords increase the risk of further breaches.
- **Geographical exposure:** The dump is categorized by country, making it easier for threat actors to target specific regions.
- **IP Address Context:** Each folder in the leaked dump includes IP addresses linked to individual configurations, making it simpler for attackers to target and exploit devices.

Top Countries Affected

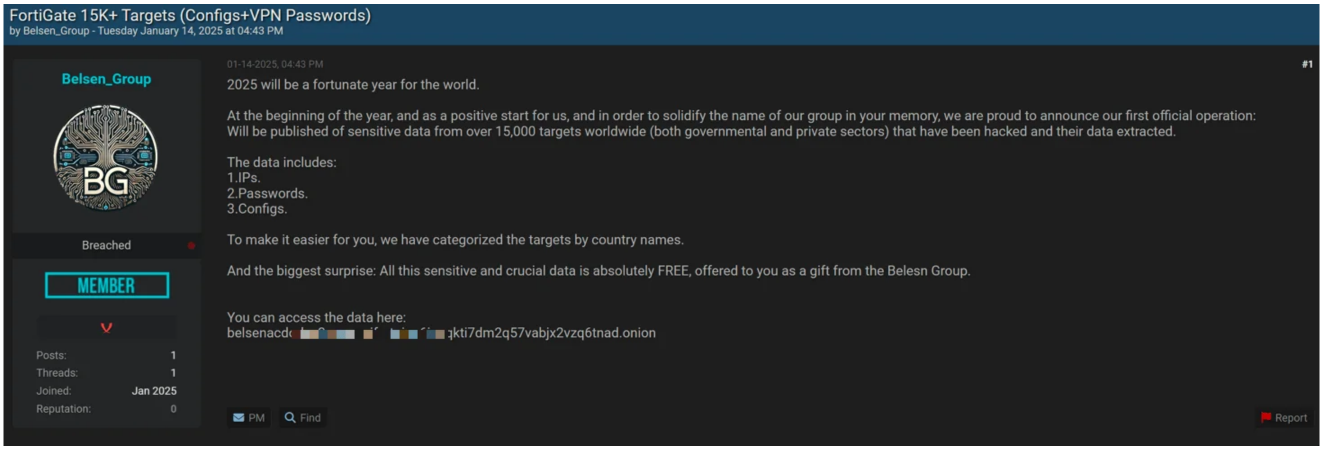
Through analysis of the affected IP addresses, SOCRadar identified the top countries impacted by this breach. Mexico and the United Arab Emirates led the list, with **1,603 devices (10.34%)** and **1,081 devices (6.98%)** affected, respectively. Notably, the top 10 affected countries accounted for more than **51%** of the impacted devices across the **144 affected countries**. The remaining top 10 countries, including Thailand, Malaysia, and the United States, are displayed in the accompanying graph.



This data showcases the widespread nature of the exploit, leaving organizations across various regions vulnerable to potential attacks.

Similarities to CVE-2024-55591

The recent disclosure of CVE-2024-55591 underscores the ongoing risks associated with Fortinet devices. While the security researcher Kevin Beaumont confirmed that the Belsen Group exploited CVE-2022-40684 to gain access to and leak FortiGate configurations, he also warned that similar threat actors may target the newly discovered CVE-2024-55591. Despite their technical differences, both vulnerabilities exposed critical administrative controls on Fortinet systems, allowing attackers to make unauthorized configuration changes and compromise VPN credentials.



FortiGate 15K+ Targets (Configs+VPN Passwords)
by Belsen_Group - Tuesday January 14, 2025 at 04:43 PM

Belsen_Group

Breached

MEMBER

Posts:	1
Threads:	1
Joined:	Jan 2025
Reputation:	0

01-14-2025, 04:43 PM #1

2025 will be a fortunate year for the world.

At the beginning of the year, and as a positive start for us, and in order to solidify the name of our group in your memory, we are proud to announce our first official operation:
Will be published of sensitive data from over 15,000 targets worldwide (both governmental and private sectors) that have been hacked and their data extracted.

The data includes:
1.IPs.
2.Passwords.
3.Configs.

To make it easier for you, we have categorized the targets by country names.

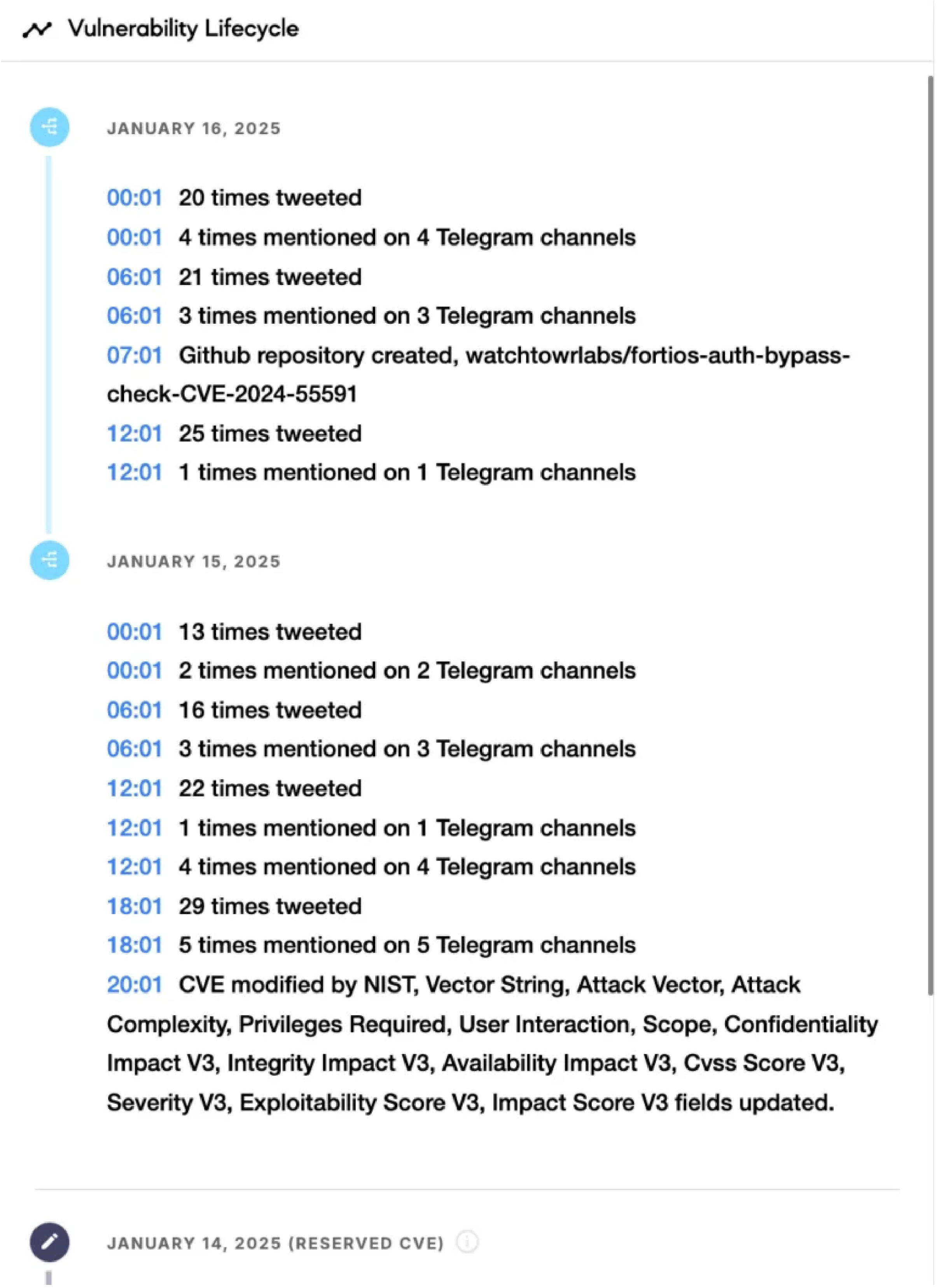
And the biggest surprise: All this sensitive and crucial data is absolutely FREE, offered to you as a gift from the Belesn Group.

You can access the data here:
belsenacd[redacted]kti7dm2q57vabjx2vzq6tnad.onion

Dark web announcement by Belsen Group showcasing leaked configurations and credentials

Kaushík Pał emphasized the importance of patching both vulnerabilities, noting that attackers who exploited the 2022 zero-day may already be planning how to exploit CVE-2024-55591. This is consistent with broader trends in the cybersecurity landscape, in which advanced threat actors frequently repurpose successful methodologies for new vulnerabilities to broaden their attack scope. Both incidents highlight the importance of securing administrative interfaces, applying patches quickly, and constantly monitoring for signs of compromise.

According to the lifecycle findings in SOCRadar’s Vulnerability Intelligence module, CVE-2024-55591 has gained attention on social platforms like Telegram, where it has been mentioned multiple times across different channels.



Vulnerability Lifecycle

JANUARY 16, 2025

00:01 20 times tweeted
00:01 4 times mentioned on 4 Telegram channels
06:01 21 times tweeted
06:01 3 times mentioned on 3 Telegram channels
07:01 Github repository created, watchtowrlabs/fortios-auth-bypass-check-CVE-2024-55591
12:01 25 times tweeted
12:01 1 times mentioned on 1 Telegram channels

JANUARY 15, 2025

00:01 13 times tweeted
00:01 2 times mentioned on 2 Telegram channels
06:01 16 times tweeted
06:01 3 times mentioned on 3 Telegram channels
12:01 22 times tweeted
12:01 1 times mentioned on 1 Telegram channels
12:01 4 times mentioned on 4 Telegram channels
18:01 29 times tweeted
18:01 5 times mentioned on 5 Telegram channels
20:01 CVE modified by NIST, Vector String, Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality Impact V3, Integrity Impact V3, Availability Impact V3, Cvss Score V3, Severity V3, Exploitability Score V3, Impact Score V3 fields updated.

JANUARY 14, 2025 (RESERVED CVE)

SOCRadar’s Vulnerability Intelligence module Vulnerability Lifecycle

The timeline shows a significant increase in discussions and activity related to this vulnerability, indicating growing interest from users—and potentially threat actors. This highlights the urgency for organizations to monitor such developments and act swiftly to protect their systems.

Lessons Learned: Patch and Monitor

Even if organizations patched CVE-2022-40684 in late 2022, the stolen data may have already been exfiltrated and exploited. This emphasizes the importance of proactive patch management and monitoring for Indicators of Compromise (IoCs). Logs should be examined for suspicious activity, such as:

- **user=”Local_Process_Access”**
- **user_interface=”Node.js” or “Report Runner”**

Mitigation and Next Steps

To mitigate the risks associated with this breach, organizations should:

1. **Change device credentials** immediately for all affected Fortinet devices.
2. **Reassess firewall rules** to identify potential vulnerabilities revealed by the leaked configurations.
3. **Implement additional security layers**, such as IP restrictions and disabling public-facing administrative interfaces.
4. **Adopt proactive vulnerability intelligence platforms** like SOCRadar to monitor exposed data and mitigate risks.

Fortinet’s Official Statement on the Breach

Fortinet has issued a detailed statement responding to the Belsen Group’s recent claims about leaked FortiGate firewall configurations and VPN credentials. According to their analysis, the data comes from older campaigns that exploited CVE-2022-40684, not any recent vulnerabilities or incidents. The exposed data, organized by country and IP address, primarily consists of configurations from FortiOS 7.0.6 and 7.2.1, the last vulnerable versions before patches were released in 2022.

According to Fortinet’s investigation, the leaked data also includes IoCs related to previous vulnerabilities, such as FG-IR-22-377 and FG-IR-18-384, indicating that the threat actor repackaged outdated information to appear as a new disclosure. Organizations that have consistently followed Fortinet’s best practices, such as upgrading to supported versions of FortiOS and refreshing credentials, are at low risk from this vulnerability. Fortinet also confirmed that devices purchased after December 2022 or running FortiOS 7.2.2 and higher are unaffected by the leak.

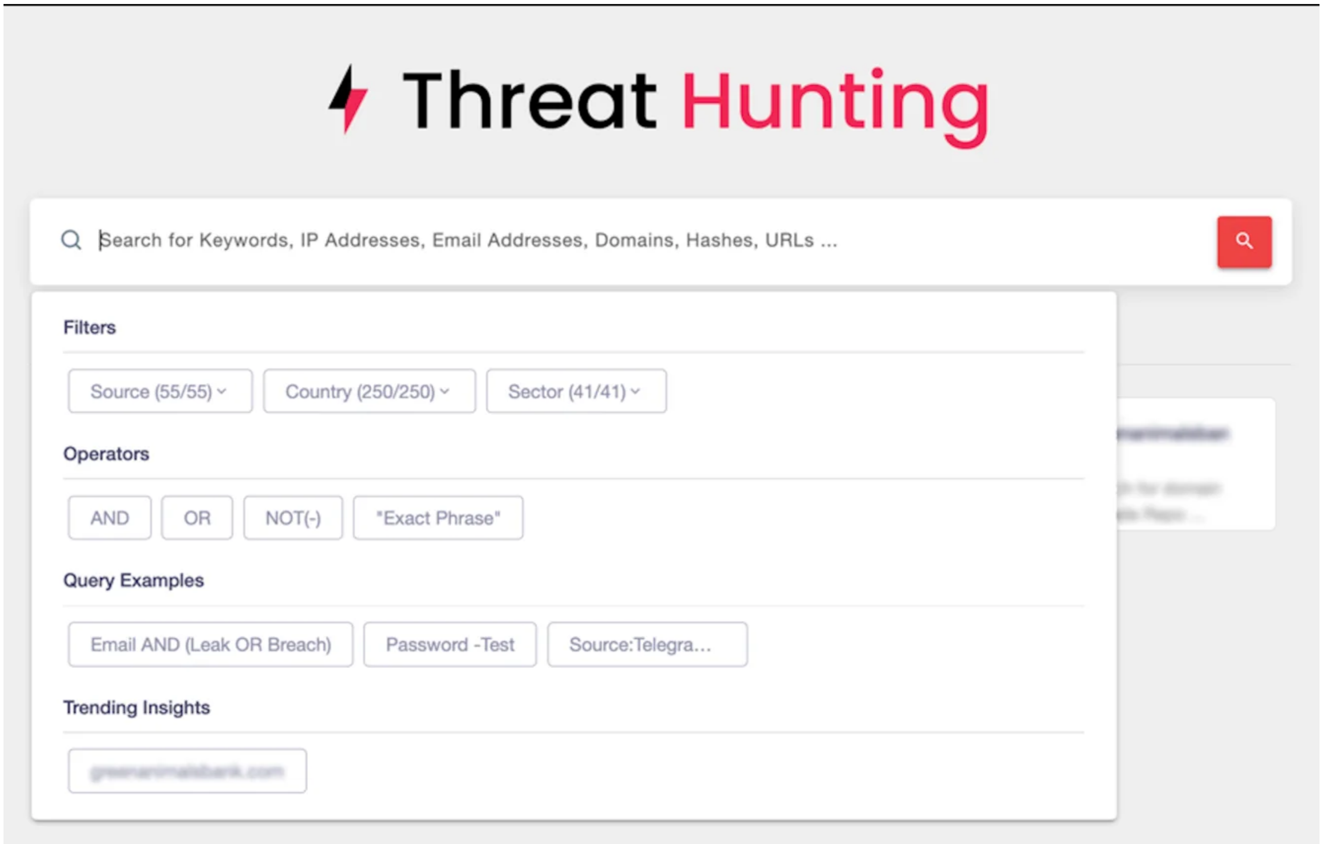
Recommended Actions by Fortinet:

1. Ensure your FortiGate devices are updated to the latest FortiOS versions.

2. Validate configurations for unauthorized changes using Fortinet’s detailed IoCs.
3. Adhere to routine credential-refreshing practices.

Boost Your Cyber Defense with SOCRadar’s Threat Hunting Module

In a space where advanced threats and zero-day vulnerabilities can go undetected for months, proactive threat hunting is no longer an option; it’s required. **SOCRadar’s Threat Hunting** module enables organizations to identify hidden threats before they escalate. Security teams can quickly identify malicious activities and improve incident response capabilities by leveraging actionable intelligence, automated IOC searches, and advanced correlation techniques.



Track and investigate emerging threats in real time with SOCRadar’s Threat Hunting module

SOCRadar provides real-time insights and in-depth analytics to help your team stay ahead of evolving cyber threats such as the recent FortiGate exploits. With SOCRadar’s Threat Hunting module, you can proactively defend your digital ecosystem rather than waiting for the next breach. Explore how it can improve your security operations today.

Looking Forward

The FortiGate exploit highlights the enduring danger of delayed patching and the long-term consequences of zero-day vulnerabilities. With over 15,000 firewalls exposed, the need for continuous monitoring, robust incident response plans, and comprehensive cybersecurity measures has never been clearer. Tools like **SOCRadar Vulnerability Intelligence** can play a critical role in helping organizations stay informed and secure against evolving threats.

PROTECTION OF PERSONAL DATA COOKIE POLICY FOR THE INTERNET SITE

Protecting your personal data is one of the core principles of our organization, SOCRadar, which operates the internet site (www.socradar.com). This Cookie Usage Policy ("Policy") explains the types of cookies used and the conditions under which they are used to all website visitors and users.

Cookies are small text files stored on your computer or mobile device by the websites you visit.

Cookies are commonly used to provide you with a personalized experience while using a website, enhance the services offered, and improve your overall browsing experience, contributing to ease of use while navigating a website. If you prefer not to use cookies, you can delete or block them through your browser settings. However, please be aware that this may affect your usage of our website. Unless you change your cookie settings in your browser, we will assume that you accept the use of cookies on this site.

1. WHAT KIND OF DATA IS PROCESSED IN COOKIES?

Cookies on websites collect data related to your browsing and usage preferences on the device you use to visit the site, depending on their type. This data includes information about the pages you access, the services and products you explore, your preferred language choice, and other preferences.

2. WHAT ARE COOKIES AND WHAT ARE THEIR PURPOSES?

Cookies are small text files stored on your device or web server by the websites you visit through your browsers. These small text files, containing your preferred language and other settings, help us remember your preferences on your next visit and assist us in making improvements to our services to enhance your experience on the site. This way, you can have a better and more personalized user experience on your next visit.

The main purposes of using cookies on our Internet Site are as follows:

- Improve the functionality and performance of the website to enhance the services provided to you,
- Enhance and introduce new features to the Internet Site and customize the provided features based on your preferences,
- Ensure legal and commercial security for the Internet Site, yourself, and the Organization, and prevent fraudulent transactions through the Site,
- Fulfill legal and contractual obligations, including those arising from Law No. 5651 on the Regulation of Publications on the Internet and the Fight Against Crimes Committed Through These Publications, as well as the Regulation on the Procedures and Principles Regarding the Regulation of Publications on the Internet.

3. TYPES OF COOKIES USED ON OUR INTERNET SITE 3.1. Session Cookies

Session cookies ensure the smooth operation of the internet site during your visit. They are used for purposes such as ensuring the security and continuity of our sites and your visits. Session cookies are temporary cookies and are deleted when you close your browser; they are not permanent.

3.2. Persistent Cookies

These cookies are used to remember your preferences and are stored on your device through browsers. Persistent cookies remain stored on your device even after you close your browser or restart your computer. These cookies are stored in your browser’s subfolders until deleted from your browser’s settings. Some types of persistent cookies can be used to provide personalized recommendations based on your usage purposes.

With persistent cookies, when you revisit our website with the same device, the website checks if a cookie created by our website exists on your device. If so, it is understood that you have visited the site before, and the content to be presented to you is determined accordingly, offering you a better service.

3.3. Mandatory/Technical Cookies

Mandatory cookies are essential for the proper functioning of the visited internet site. The purpose of these cookies is to provide necessary services by ensuring the operation of the site. For example, they allow access to secure sections of the internet site, use of its features, and navigation.

3.4. Analytical Cookies

These cookies gather information about how the website is used, the frequency and number of visits, and show how visitors navigate to the site. The purpose of using these cookies is to improve the operation of the site, increase its performance, and determine general trend directions. They do not contain data that can identify visitors. For example, they show the number of error messages displayed or the most visited pages.

3.5. Functional Cookies

Functional cookies remember the choices made by visitors within the site and recall them during the next visit. The purpose of these cookies is to provide ease of use to visitors. For example, they prevent the need to re-enter the user's password on each page visited by the site user.

3.6. Targeting/Advertising Cookies

They measure the effectiveness of advertisements shown to visitors and calculate how many times ads are displayed. The purpose of these cookies is to present personalized advertisements to visitors based on their interests.

Similarly, they determine the specific interests of visitors' navigation and present appropriate content. For example, they prevent the same advertisement from being shown again to the visitor in a short period.

4. HOW TO MANAGE COOKIE PREFERENCES?

To change your preferences regarding the use of cookies, block or delete cookies, you only need to change your browser settings.

Many browsers offer options to accept or reject cookies, only accept certain types of cookies, or receive notifications from the browser when a website requests to store cookies on your device.

Also, it is possible to delete previously saved cookies from your browser.

If you disable or reject cookies, you may need to manually adjust some preferences, and certain features and services on the website may not work properly as we will not be able to recognize and associate with your account. You can change your browser settings by clicking on the relevant link from the table below.

5. EFFECTIVE DATE OF THE INTERNET SITE PRIVACY POLICY

The Internet Site Privacy Policy is dated The effective date of the Policy will be updated if the entire Policy or specific sections are renewed. The Privacy Policy is published on the Organization's website (www.socradar.com) and made accessible to relevant individuals upon request.

SOCRadar
Address: 651 N Broad St, Suite 205 Middletown, DE 19709 USA
Phone: +1 (571) 249-4598
Email: [email protected]
Website: www.socradar.com