مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Fortinet FortiGate Firewall Data Leak

Tracking #:432316759

Date:17-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a threat actor named "Belsen Group" has published data allegedly from 15,000 Fortinet FortiGate firewall instances on the dark web and Fortinet's analysis reveals that this data is not from a new breach but a resharing of information obtained from previous incidents prior to November 2022.

TECHNICAL DETAILS:

A threat actor named "Belsen Group" has published data allegedly from 15,000 Fortinet FortiGate firewall instances on the dark web. Fortinet's analysis reveals that this data is not from a new breach but a resharing of information obtained from previous incidents prior to November 2022. The leaked data primarily relates to two older vulnerabilities: CVE-2022-40684 and CVE-2018-13379. The data includes older firmware versions and configurations (such as **FortiOS 7.0.6** and **7.2.1**), which were addressed in past advisories. While organizations with outdated configurations or those not adhering to best practices may still be at risk, Fortinet assures that the majority of devices in use today are not impacted.

A threat actor, recently surfaced in January 2025, posted files containing **FortiGate** data on a dark web forum, claiming the data was stolen from FortiGate devices. The data in question includes:

- **IPs**
- **Passwords**
- **Configurations**

Fortinet's analysis reveals the data includes configurations and VPN credentials linked to **older FortiOS versions** (specifically **7.0.6**, **7.2.1**, and earlier). These versions are tied to vulnerabilities that were previously disclosed and patched by Fortinet.

Key Findings:

1. **Config Data (config.conf):**
   - The **config.conf** files found in the threat actor's posting show FortiGate configurations associated with **SSL-VPN ports (443, 10443)**.
   - The configurations correspond to FortiOS versions that are **older than 7.6**, specifically **7.2.1** and **7.0.6**, which were addressed in earlier vulnerabilities.
   - The presence of known **Indicators of Compromise (IoCs)**, such as configurations linked to **CVE-2022-40684**, suggests that this data was obtained from past incidents and not from recent breaches.
2. **VPN Credentials (vpn-password.txt):**
   - The **vpn-password.txt** files contain SSL-VPN credentials from FortiGate devices. These credentials match the data disclosed in a prior vulnerability, **CVE-2018-13379** (also known as the SSL-VPN credential leak).
   - The filenames and headers were altered by the threat actor, suggesting an attempt to make the files appear more recent.
3. **Malicious Access Indicators:**
   - Malicious admin indicators (e.g., **fortigate-tech-support**) and evidence of **Local_Process_Access** further corroborate that the data was obtained through earlier exploits that had already been patched.

Impacted Devices:

- FortiGate devices running FortiOS 7.0.6 or earlier prior to November 2022.
- FortiGate devices running FortiOS 7.2.1 or earlier prior to November 2022.
- Devices purchased before December 2022 that may still be using vulnerable versions of FortiOS (if not updated).

Non-Impacted Devices:

- Devices purchased since December 2022 or those running FortiOS 7.2.2 or later are not affected by the disclosed data.
- Devices that have been regularly patched and updated and adhere to best practices should not be at significant risk.

RECOMMENDATIONS:

1. Upgrade to the Latest FortiOS Version:
   - Immediately upgrade all FortiGate devices to the latest FortiOS version, especially for devices on versions 7.0.6, 7.2.1, or earlier. The latest patches address past vulnerabilities such as CVE-2022-40684 and CVE-2018-13379.
2. Review Device Configuration:
   - Validate that your device configurations are current and secure, with no unauthorized changes.
   - Device running a vulnerable version, review the config.conf files and vpn-password.txt files to check for any signs of compromise.
3. Refresh Security Credentials:
   - Regularly refresh VPN credentials and ensure that passwords are strong, unique, and regularly updated.
   - Ensure that any previous credentials associated with outdated configurations are no longer in use.
4. Consult Known Indicators of Compromise (IoCs):
   - Review the IoCs shared in the past advisories (such as FG-IR-22-377 and FG-IR-18-384) and cross-reference any known indicators in your systems.
   - Look for signs of malicious access attempts tied to known vulnerabilities.
5. Follow Fortinet Best Practices:
   - Follow best practice recommendations provided by Fortinet in prior advisories to strengthen the security of your FortiGate deployments.
   - Regularly check for new Fortinet advisories and security updates.
6. Contact Fortinet Support:
   - Fortinet customer may reach out to Fortinet support at cs@fortinet.com for further assistance.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.fortinet.com/blog/psirt-blogs/analysis-of-threat-actor-data-posting