Serianu Cyber Security Advisory

CVE-2018-13379 (FG-IR-18-384) | FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests

Serianu SOC Advisory Number:

TA – 2020/022

Date(s) issued:

27th November, 2020

System Affected:

Fortinet SSL VPN

Overview:

Serianu Cyber Threat Intelligence research team discovered a threat actor that scans the internet and identifies a list of FortiGate devices which have not been upgraded since publication of **CVE-2018-13379 (FG-IR-18-384) | FortiOS (**Fortinet's Network Operating System **)system file leak through SSL VPN via specially crafted HTTP resource requests**.

A path traversal vulnerability in the FortiOS SSL VPN web portal could allow an unauthenticated attacker to download FortiOS system files through specially crafted HTTP resource requests. This vulnerability was fixed in 2019 in FortiOS 5.4.13, 5.6.8, 6.0.5 or 6.2.0 and above and it exists when SSL VPN service (web mode/tunnel mode) is enabled.

Serianu continues to remind organisations that it's critical to keep FortiGate devices running the latest patch in order to be up-to-date with the latest security fixes. Security is our first priority and we continue to proactively communicate and advice organisations.

Description

FortiOS is a security-hardened, purpose-built operating system that is the software foundation of FortiGate. It controls all the security and networking capabilities in all FortiGates across the entire network with a friendly and easy to use operating system.

- The FortiOS provides the IT teams with a visibility into devices, traffic, applications and events and the ability to detect and stop a threat through centralized analytics.

A **Secure Sockets Layer Virtual Private Network** (SSL VPN) is a virtual private network (VPN) created using the Secure Sockets Layer (SSL) protocol to create a secure and encrypted connection over a less-secure network.

Impact

1. Information Disclosure: The attacker can read any files (including system critical files like: config files/password files) from the server.
2. Attackers can perform trial and error (problem solving technique in which multiple attempts are made to reach a solution) to search and read sensitive files on the target server.
3. Malicious actors can exploit this vulnerability and cause serious downtime resulting in significant financial loss.
4. Since VPN endpoints play a crucial role in a business infrastructure, compromise of even a single endpoint may lead to take over of the entire domain or network.

Affected Products

1. FortiOS 6.0 - 6.0.0 to 6.0.4
2. FortiOS 5.6 - 5.6.3 to 5.6.7
3. FortiOS 5.4 - 5.4.6 to 5.4.12

(other branches and versions than above are not impacted)
ONLY if the SSL VPN service (web-mode or tunnel-mode) is enabled.

Workarounds

As a temporary solution, the only workaround is to totally DISABLE the SSL-VPN service (both web-mode and tunnel-mode) by applying the following CLI commands:

config vpn ssl settings
unset source-interface
end

Please note, firewall policies tied to SSL VPN will need to be unset first for the above sequence to execute successfully. For example, when source-interface is "port1" and SSL VPN interface is "ssl.root", the following CLI commands would be needed to ensure "unset source-interface" executes successfully:

config vpn ssl settings
config authentication-rule
purge (purge all authentication-rules)
end
end
config firewall policy
delete [policy-id] (SSL VPN policy ID(s) that srcintf is "ssl.root" and dstintf is "port1")
end

Recommendations

1. Upgrade to FortiOS 5.4.13, 5.6.8, 6.0.5 or 6.2.0 and above.
2. Due to the ability to exploit this issue remotely and that threat actors actively target this vulnerability, Serianu is strongly recommending all organisations with the vulnerable versions to perform an immediate upgrade.
3. FortiGuard signatures to be deployed to monitor attack traffic in the wild and enable a FortiGuard response.
4. Enabling two-factor authentication for SSL VPN users

Conclusion

The code to exploit this vulnerability in order to obtain the credentials of logged in SSL VPN users was disclosed. In absence of upgrading to the versions listed above, mitigating the impact of this exploit can be done by enabling two-factor authentication for SSL VPN users. An attacker would then not be able to use stolen credentials to impersonate SSL VPN users.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organization or individual that has access to commonly exploited vulnerabilities to share it with us through our email info@serianu.com to allow us to analyze any indicators of compromise (IOC).