Mphasis
The Next Applied

Fortinet fixes critical RCE flaw in FortiGate Firewalls

Severity: High

Description

Fortinet has released patches to address a critical security flaw in its FortiGate firewalls that could be abused by a threat actor to achieve remote code execution. The security fixes were released in FortiOS firmware versions 6.0.17, 6.2.15, 6.4.13, 7.0.12, and 7.2.5.

Technical details

Fortinet devices are some of the most popular firewall and VPN devices in the market, making them a popular target for attacks. Over 250,000 FortiGate firewalls can be reached from the Internet, and as this bug affects all previous versions, the majority are likely exposed.

The flaw would allow a hostile agent to interfere via the VPN, even if the MFA is activated. In the past, SSL-VPN flaws have been exploited by threat actors just days after patches are released, commonly used to gain initial access to networks to conduct data theft and ransomware attacks.

Recommendation

The security fixes were released on Friday in FortiOS firmware versions 6.0.17, 6.2.15, 6.4.13, 7.0.12, and 7.2.5. Admins must apply Fortinet security updates as soon as they become available.

Reference Links

Fortinet fixes critical RCE flaw in Fortigate SSL-VPN devices, patch now (bleepingcomputer.com)

Critical RCE Flaw Discovered in Fortinet FortiGate Firewalls - Patch Now! (ampproject.org)

Copyright © Mphasis Corporation. All rights reserved.