FortiGate Vulnerability

FortiGate has identified a remote code execution and DDoS vulnerability (CVE-2023-25610) affecting their firewall appliances. This exploit could enable malicious actors to execute arbitrary code, and launch Denial of Service attacks targeting firewall interfaces. FortiGate has classified the severity as "Critical" with a CVSSv3 (Common Vulnerability Scoring System) score of 9.3 out 10.

The vendor's recommended remediation is to immediately upgrade affected firewalls to the latest firmware release. Given the severity of this vulnerability, it's potential to permit harm, and the limited disruption associated with its remediation (under normal circumstances), we began proactively pro-actively updating FortGate firewalls in use by our recurring service customers as of this morning.

Further information regarding this vulnerability is available on the FortiGuard website via the link below, and via the National Institute for Standards and Technology website also provided. Should you have questions or desire confirmation that your specific environment has been updated or is slated for updating, you may respond to this email or contact our support helpdesk at 424-207-5140.

FortiGate: PSIRT Advisories | FortiGuard

NIST: NVD - CVE-2023-25605 (nist.gov)

Sincerely,

Chris Harper
Chief Security Officer
Sandbox Technologies, Inc.