TLP: WHITE

Advisory Alert

Alert Number : **AAA20210208** **Date :** **February 8, 2021**

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	High	Multiple Vulnerabilities

Description

Affected Product	Fortinet
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-29019,CVE-2020-29018, CVE-2020-29017 , CVE-2020-29016,CVE-2020-29015,CVE-2018-13381, CVE-2018-13383, CVE-2021-22122)
Description	Fortinet has fixed critical vulnerabilities including Privilege escalation, remote code execution, SQL injections, buffer overflows, and denial of service attacks identified in SSL VPN and web firewall. **CVE-2020-29019**: A stack-based buffer overflow vulnerability in FortiWeb allows a remote, unauthenticated attacker to crash the httpd service thread by sending a request with a crafted cookie header. **CVE-2020-29018**: A format string vulnerability in FortiWeb allows an authenticated, remote attacker to read the contents of memory and retrieve sensitive data via the redir parameter. **CVE-2020-29017**: An OS command injection vulnerability in FortiDeceptor allows a remote authenticated attacker to execute arbitrary commands. **CVE-2020-29016**: A stack-based buffer overflow vulnerability in FortiWeb allows an unauthenticated, remote attacker to overwrite the content of the stack and potentially execute arbitrary code by sending a crafted request with a large certname. **CVE-2020-29015**: A blind SQL injection in the user interface of FortiWeb may allow an unauthenticated, remote attacker to execute arbitrary SQL queries with a crafted Authorization header containing a malicious SQL statement. **CVE-2018-13381**: Failure to properly parse message payloads in the SSL VPN portal of FortiOS may allow a non-authenticated attacker to perform a Denial of Service attack via exploiting a buffer overflow. **CVE-2018-13383**: A heap buffer overflow vulnerability in the FortiOS SSL VPN web portal may cause the SSL VPN web service termination for logged in users or potential remote code execution on FortiOS **CVE-2021-22122**: An improper neutralization of input during web page generation in FortiWeb GUI interface may allow an unauthenticated, remote attacker to perform a reflected cross-site scripting attack
Affected Products	FortiWeb 6.3.7 and below, 6.2.3 and below FortiWeb 6.3.5 and below FortiDeceptor 3.1.0 and below, 3.0.1 and below. FortiWeb 6.3.5 and below, 6.2.3 and below FortiWeb 6.3.7 and below, 6.2.3 and below. FortiProxy SSL VPN 2.0.0 and below, 1.2.8 and below, 1.1.6 and below, 1.0.7 and below. FortiProxy SSL VPN 2.0.0 and below, 1.2.8 and below, 1.1.6 and below, 1.0.7 and below. FortiOS 6.0.0 to 6.0.4 FortiOS 5.6.0 to 5.6.10 FortiOS 5.4.0 to 5.4.12 FortiOS 5.2.0 to 5.2.14 Branch lower than 5.2 not been assessed.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-20-126 https://www.fortiguard.com/psirt/FG-IR-20-123 https://www.fortiguard.com/psirt/FG-IR-20-125 https://www.fortiguard.com/psirt/FG-IR-20-124 https://www.fortiguard.com/psirt/FG-IR-18-387 https://www.fortiguard.com/psirt/FG-IR-18-388 https://www.fortiguard.com/psirt/FG-IR-18-388 https://www.fortiguard.com/psirt/FG-IR-20-122

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.