The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
01/06/2021

SUBJECT:
Multiple Vulnerabilities in Fortinet FortiWeb Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in the Fortinet FortiWeb, the most severe of which could allow for arbitrary code execution. Fortinet FortiWeb is a firewall for web applications which provides threat protection for medium and large enterprises. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution within the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- FortiWeb versions 6.3.7 and below.
- FortiWeb versions 6.2.3 and below.

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Fortinet FortiWeb, the most severe of which could allow for arbitrary code execution within the context of a privileged process. Details of these vulnerabilities are as follows:

- A blind SQL injection in the user interface of FortiWeb may allow an unauthenticated, remote attacker to execute arbitrary SQL queries or commands by sending a request with a crafted Authorization header containing a malicious SQL statement. (CVE-2020-29015)
- A stack-based buffer overflow vulnerability in FortiWeb may allow 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-2020-29016)
- A format string vulnerability in FortiWeb may allow an authenticated, remote attacker to read the content of memory and retrieve sensitive data via the redir parameter. (CVE-2020-29018)
- A stack-based buffer overflow vulnerability in FortiWeb may allow a remote, authenticated attacker to crash the httpd daemon thread by sending a request with a crafted cookie header. (CVE-2020-29019)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution within the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates by Fortinet to vulnerable systems, immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments, especially from un-trusted sources.

REFERENCES:

FortiGuard:

https://www.fortiguard.com/psirt/FG-IR-20-123
https://www.fortiguard.com/psirt/%20FG-IR-20-124
https://www.fortiguard.com/psirt/FG-IR-20-125
https://www.fortiguard.com/psirt/%20FG-IR-20-126

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29019