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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
11/22/2021

SUBJECT:
A Vulnerability in Fortinet FortiWeb Could Allow for Arbitrary Code Execution.

OVERVIEW:
A vulnerability has been discovered in Fortinet FortiWeb that 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 this vulnerability 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 this vulnerability could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- FortiWeb versions prior to 6.4.1
- FortiWeb versions prior to 6.3.16
- FortiWeb versions prior 6.2.6

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Fortinet FortiWeb, that could allow for arbitrary code execution. This vulnerability can be exploited when an unauthenticated attacker overwrites the content of the stack by sending crafted HTTP requests with large request parameter values.

Successful exploitation of this vulnerability 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 this vulnerability 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-21-119

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36186

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.