*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**
**www.cisa.gov/tlp**
**Information may be distributed without restriction, subject to standard copyright rules.**

**DATE(S) ISSUED:**
10/11/2022

**SUBJECT:**
A Vulnerability in FortiOS / FortiProxy / FortiSwitchManager Could Allow for Authentication Bypass

**OVERVIEW:**
A vulnerability has been discovered in FortiOS, FortiProxy and FortiSwitchManager, which could allow for authentication bypass on administrative interface. FortiOS is the Fortinet's proprietary Operation System which is utilized across multiple product lines. FortiProxy is a secure web proxy that protects employees against internet-borne attacks by incorporating multiple detection techniques. FortiSwitch Manager is an on-premise management platform for the FortiSwitch product. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

**THREAT INTELLIGENCE:**
Fortinet is aware of instances where there is an exploitation against the vulnerability.

**SYSTEMS AFFECTED:**

- FortiOS version 7.2.0 through 7.2.1
- FortiOS version 7.0.0 through 7.0.6
- FortiProxy version 7.2.0
- FortiProxy version 7.0.0 through 7.0.6
- FortiSwitchManager version 7.2.0
- FortiSwitchManager version 7.0.0

**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: Low**

**TECHNICAL SUMMARY:**
A vulnerability has been discovered in FortiOS, FortiProxy and FortiSwitchManager, which could allow for authentication bypass on administrative interface. Details of this vulnerability are as follows:

**Tactic**: *Initial Access* (TA0001):

**Technique**: *Exploit Public Facing Application* (T1190):

- CVE-2022-40684 - An authentication bypass using an alternate path or channel vulnerability [CWE-288] in FortiOS, FortiProxy and FortiSwitchManager may allow an unauthenticated atttacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests.

Successful exploitation of this vulnerability could allow for arbitrary code execution in the context of the logged on user. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply appropriate updates or workarounds provided by Fortinet to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
- Restrict execution of code to a virtual environment on or in transit to an endpoint system. (**M1048: Application Isolation and Sandboxing**)
    - **Safeguard 4.1: Establish and Maintain a Secure Configuration Process**: Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 16.8: Separate Production and Non-Production Systems:** Maintain separate environments for production and non-production systems.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)
    - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.
    - **Safeguard 13.10: Performing Application Layer Filtering:** Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.

- Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc. (**M1021: Restrict Web-Based Content**)
    - **Safeguard 9.2: Use DNS Filtering Services:** Use DNS filtering services on all enterprise assets to block access to known malicious domains.
    - **Safeguard 9.3: Maintain and Enforce Network-Based URL Filters:** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
    - **Safeguard 9.6: Block Unnecessary File Types:** Block unnecessary file types attempting to enter the enterprise's email gateway.

- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources. Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. (**M1017: User Training**)
    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

**REFERENCES:**

**Fortinet:**https://www.fortiguard.com/psirt/FG-IR-22-377

**Bleeping Computer:**
https://www.bleepingcomputer.com/news/security/fortinet-warns-admins-to-patch-critical-auth-bypass-bug-immediately/

**CVE:**
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40684