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:
03/28/2022

SUBJECT:
A Vulnerability in Sophos Firewall Could Allow for Arbitrary Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Sophos Firewall's user portal and Webadmin that could allow for arbitrary remote code execution. Sophos Firewall is a next generation firewall product which enables users to manage, detect and respond to threats on the network. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code in the context of the web application. Depending on the privileges associated with the application, an attacker could view, change, or delete data.

THREAT INTELLIGENCE:
Sophos is aware of this vulnerability currently being exploited in a small set of organizations located in the Southern Asia region.

SYSTEMS AFFECTED:

- Sophos Firewall v18.5 MR3 (18.5.3) and older

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 authentication bypass vulnerability has been discovered in Sophos Firewall's user portal and Webadmin that could allow for arbitrary remote code execution. Sophos Firewall is a next generation firewall product which enables users to manage, detect and respond to threats on the network. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code in the context of the web application. Depending on the privileges associated with the application, an attacker could view, change, or delete data.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply updates provided by Sophos to vulnerable systems immediately after appropriate testing.
- Disable WAN access to the User Portal and Webadmin
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Sophos:https://www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce

CVE:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1040