Hive Pro

# THREAT ADVISORY

## Sophos Firewall RCE vulnerability actively exploited

**TA2022082**

**Threat Level** AMBER

**Publish Date –** March 30, 2022

A security researcher has discovered an authentication bypass vulnerability that resides in the User Portal and Webadmin areas of Sophos Firewall. Attackers are actively exploiting this vulnerability to attack enterprises in South Asia.

The vulnerability, tracked as CVE-2022-1040, allows a remote attacker with access to the Firewall's User Portal or Webadmin user to circumvent authentication and execute arbitrary code.

Sophos published hotfixes to address this vulnerability, which has been automatically deployed to all susceptible devices because the 'Allow automatic installation of hotfixes' functionality that is activated by default. However, hotfixes published for end-of-life Sophos Firewall versions must be manually upgraded in order to address the security issue and defend against ongoing assaults. Customers can also defend themselves from external attackers by not exposing their User Portal and Webadmin to the WAN.

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
TA0006: Credential Access
TA0007: Discovery
TA0001: Initial Access
TA0004: Privilege Escalation
TA0005: Defense Evasion
T1588: Obtain Capabilities
T1588.006: Obtain Capabilities: Vulnerabilities
T1190: Exploit Public-Facing Application
T1040: Network Sniffing
T1548: Abuse Elevation Control Mechanism

### Vulnerability Details

| CVE ID | Affected Products | Affected CPE | Vulnerability Name | CWE ID |
|---|---|---|---|---|
| CVE-2022-1040 | Sophos Firewall v18.5 MR3 (18.5.3) and older | cpe:2.3:o:sophos:xg_firewall_firmware:*:*:*:*:*:*:*:* | An authentication bypass vulnerability in the User Portal and Webadmin | CWE-287 |

### References

https://www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce
https://support.sophos.com/support/s/article/KB-000043853?language=en_US