Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 165 **19-01-2023**

Name: Sophos Firewall Devices Vulnerable to Critical RCE Vulnerability (CVE-2022-3236)

Threat Classification: Remote Code Execution (RCE)

Affected Versions: v19.0 MR1/19.0.1 and older

Summary:

A critical remote code execution (RCE) vulnerability (CVE-2022-3236) has been found in the User Portal and Webadmin of Sophos Firewall. The vulnerability has been exploited in the wild in attacks against organizations from South Asia. Sophos has released hotfixes for multiple Sophos Firewall versions, however, thousands of devices are still vulnerable.

Severity	**High**
Attack Vector	**Network**
Privileges required	**Low**

Recommendations:

- Upgrade Sophos Firewall instances to a supported version to receive the hotfix automatically.
- Remove the attack surface by disabling WAN access to the User Portal and Webadmin.
- Keep software updated and monitor for new updates and patches.
- In case of any incident, please report to this office, through PTA CERT Portal and email.

Reference links:

- https://community.sophos.com/kb/en-us/138726
- https://nvd.nist.gov/vuln/detail/CVE-2022-3236