- Risk Management
- Compliance
- Privacy
- Supply Chain

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security

- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response

- ICS/OT
- IoT Security

Home › Vulnerabilities

Details Disclosed for Critical Vulnerability in Sophos Appliances

By Eduard Kovacs on August 23, 2021

Organizations using security appliances from Sophos have been advised to make sure their devices are up to date after a researcher disclosed the details of a critical vulnerability patched last year.

Sophos informed customers in September 2020 that it had patched a remote code execution flaw affecting the web administration console (WebAdmin) of SG UTM devices. The issue, tracked as CVE-2020-25223, was reported to the cybersecurity firm by an external researcher, and it was fixed with the release of SG UTM v9.705 MR5, v9.607 MR7, and v9.511 MR11.

However, it appears that not all Sophos customers have patched their devices. During a recent client engagement, Justin Kennedy, research consulting director at information security consultancy Atredis Partners, noticed that the customer's UTM devices had been running a vulnerable version of the software.

Kennedy compared the differences between the patched and unpatched versions of the software, which enabled him to identify the root cause of the vulnerability.

Last week, the researcher published a blog post detailing how CVE-2020-25223 can be exploited by a remote, unauthenticated attacker for arbitrary code execution with root privileges on a Sophos appliance.

Sophos said in an emailed statement that it's not aware of any malicious attacks leveraging this vulnerability. However, Kennedy told SecurityWeek that "it would be incredibly easy for an attacker to exploit the vulnerability in a real world environment."

In order to exploit CVE-2020-25223, all an attacker needs to do is send a single HTTP request. If the WebAdmin interface is exposed to the internet, it may be possible for an attacker to exploit the vulnerability directly from the web.

Kennedy said the Shodan search engine identified over 3,100 systems that appear to expose the WebAdmin interface, but it's unclear how many of them are actually vulnerable.

He also noticed more than 95,000 instances that have the title "User Portal" instead of "WebAdmin," but he has not checked if it's possible to exploit the vulnerability or reach the exploitable path via the User Portal.

Asked if he is concerned about the information in his blog post being abused by malicious actors, the researcher noted that "if malicious actors wanted to exploit unpatched systems affected by the vulnerability, they've had more than enough time to discover the vulnerability details and exploit those systems."

He has advised organizations to check if they are still affected by this vulnerability, and if they are, to patch their systems and then review their patching policies to identify the gaps that allowed a critical vulnerability to remain unpatched for nearly a year.

Commenting on Kennedy's blog post, Sophos said, "The additional detail in the blog raises awareness about how important it is for organizations to constantly update and patch their software. The emphasis we want underscore is that updating, and patching is a critical security best practice that organizations of all sizes need to build into their ongoing maintenance routines."

It's important that organizations don't ignore these recommendations as threat actors exploiting vulnerabilities in Sophos products is not unheard of.

Related: Sophos Patches Privilege Escalation Flaws in SafeGuard Products

Related: Hackers Attempted to Deploy Ransomware in Attacks Targeting Sophos Firewalls

Related: Critical Flaw in Sophos Cyberoam Appliances Allows Remote Code Execution

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:
Details Disclosed for Critical Vulnerability in Sophos Appliances
Number of T-Mobile Customers Confirmed to Be Affected by Hack Reaches 54 Million
Google Discloses Details of Unpatched Windows AppContainer Flaw
High-Severity DoS Vulnerability Patched in BIND DNS Software
Over 600 ICS Vulnerabilities Disclosed in First Half of 2021: Report