Zero-day exploit hits Sophos Firewall XG

29 April 2020, by Peter Grad

Credit: CC0 Public Domain

Sophos rushed patches to users of its popular XG Firewall network system following reports the company received last week that hackers were actively exploiting an SQL injection vulnerability.

The assault involved the downloading and installation of a series of scripts designed to steal user names, passwords and other sensitive data.

"At this time, there is no indication that the attack accessed anything on the local networks behind any impacted XG Firewall," Team Sophos said. But they did not rule out the possibility of compromised data.

Sophos reports that the users employed a sophisticated series of steps to gain entry into systems. Taking advantage of a previously unknown SQL injection flaw, hackers were able to insert malicious code into a backend database to gain unauthorized access to protected data.

Once inside, the assault, named Asnarok by researchers, targeted administrator login credentials and remote-access user accounts. There is evidence hackers also sought firewall license and serial numbers.

"This malware's primary task appeared to be data theft, which it could perform by retrieving the contents of various database tables stored in the firewall, as well as by running some operating system commands," Sophos explained in an online report Sunday. "At each step, the malware collected information and then concatenated it to a file it stored temporarily on the firewall with the name info.xg."

Sophos determined there was "significant orchestration involved in the execution of the attack," referring to chains of Linux scripts and the utilization of apparently legitimate sites from which malware was downloaded during the attack, a process implemented each time the firewall was activated.

The Asnarok attack was first detected by a user who spotted an abnormal field entry on the system overview.

"Sophos received a report on April 22 regarding an XG Firewall with a suspicious field value visible in the management interface," the Sophos report stated. "Sophos commenced an investigation and the incident was determined to be an attack against physical and virtual XG Firewall units. The attack affected systems configured with either the administration (HTTPS service) or the User Portal exposed on the WAN zone."

If a system user's account was affected by the hack, the hot fix will display the message: "Hotfix applied for SQL injection and partially cleaned."

In those instances, Sophos recommends users reset their portal administrator and device administrator accounts, reboot the XG protected device and reset passwords for all local user accounts.

If a user's account was not compromised, the hot fix will display the message: "Hotfix applied for SQL Injection. Your device was NOT compromised."

More information:
news.sophos.com/en-us/2020/04/26/asnarok/

© 2020 Science X Network

APA citation: Zero-day exploit hits Sophos Firewall XG (2020, April 29) retrieved 17 September 2021 from https://techxplore.com/news/2020-04-zero-day-exploit-sophos-firewall-xg.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.