Attackers exploit 0-day code-execution flaw in the Sophos firewall

reader comments

43 with 31 posters participating

Share this story

Users of a widely used firewall from Sophos have been under a zero-day attack that was designed to steal usernames, cryptographically protected passwords, and other sensitive data, officials with the security firm said on Sunday.

The well-researched and developed attack exploited a SQL injection flaw in fully patched versions of the Sophos XG Firewall. With that toehold in systems, it downloaded and installed a series of scripts that ultimately executed code intended to make off with users' names, usernames, the cryptographically hashed form of the passwords, and the salted SHA256 hash of the administrator account's password. Sophos has delivered a hotfix that mitigates the vulnerability.

Other data targeted by the attack included a list of the IP address allocation permissions for firewall users; the version of the custom operating system running; the type of CPU; the amount of memory that was present on the device; how long it had been running since the last reboot; the output of the ifconfig, a command-line tool; and ARP tables used to translate IP addresses into domain names.

"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 researchers wrote in Sunday's disclosure. "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."

The exploits also downloaded the malware from domains that appeared to be legitimate. To evade detection, some of the malware deleted underlying files that executed it and ran solely in memory. The malicious code uses a creative and roundabout method to ensure it's executed each time firewalls are started. Those characteristics strongly suggest that the threat actors spent weeks or months laying the groundwork for the attacks.

Sophistication

The attack demonstrated that the attackers had a detailed knowledge of the Firewall that could only come from someone who had access to the software, which likely required a license. From there, the attackers carefully studied the Firewall to find inner workings that allowed the downloading and installation of malware that used names that closely resembled names of legitimate files and processes.

The data the malware was designed to exfiltrate suggests the attack was designed to give attackers the means to further penetrate the organizations that used the firewall through phishing attacks and unauthorized access to user accounts, and it potentially exploits targeting the firewalls or end users. The Sophos post said there was no evidence the data exfiltrations were successful, but it also didn't rule out that possibility.

The zero-day vulnerability that made the attacks possible was a pre-authentication SQL injection flaw found in the custom operating system that runs the firewall. Sophos provided no

additional details about the vulnerability. SQL injection exploit flaws that execute malicious code through strings that are entered into forms contained on a vulnerable website. The flaws are the result of a failure to filter out commands. Pre-authentication means the attacker didn’t need to provide any credentials to carry execute code.

Users of vulnerable firewalls should install the hotfix as soon as possible and then examine their systems for signs of compromise published on the previously mentioned post here.

https://arstechnica.com/?p=1671396