



Sophos XG Firewall SQLi Vulnerability Recently Exploited by Asnarök Malware

Executive Summary

Sophos XG firewall and Sophos Firewall Operating System was found to be vulnerable to SQL injection (SQLi), and was recently exploited by Asnarök Malware. The Sophos XG firewall SQLi vulnerability (CVE-020-12271) may provide an unauthenticated entry point into an IT infrastructure, and allow an attacker to exfiltrate sensitive data including plaintext usernames and hashed passwords of all local user accounts on the appliance, but not from connected systems such as Active Directory and LDAP passwords. Patches that mitigate the vulnerability are available, provided that the appliances or operating systems are supported by Sophos. HC3 encourages all updates be applied or that devices be isolated from the Internet.

Analysis

On April 22, 2020, Sophos received a report regarding an XG Firewall with a suspicious field value visible in the management interface. The incident was soon determined to be an attack against physical and virtual XG Firewall units. Sophos found affected systems that had been automatically or manually configured with either the administration interface (HTTPS admin service) or the user portal, each with firewall services exposed to the Internet.ⁱ & ⁱⁱ The attack used a previously unknown pre-authentication SQL injection (SQLi) vulnerability (CVE-2020-12271) to gain access to exposed XG devices. Asnarök malware was used in one of the detected attacks, and found to execute, then exfiltrate sensitive data, including plaintext usernames and hashed passwords of all local user accounts on the appliance, but not from connected systems such as Active Directory and LDAP passwords.

At the time of the attack, all versions (physical and virtual) of XG Firewall firmware were affected by the vulnerability (CVE-2020-12271). Sophos has deployed a hotfix for XG Firewall and SFOS to its customers, and encouraged customers running unsupported version of SFOS to upgrade immediately. Additionally it is recommended that administrators disable unneeded interfaces. Affected XG Firewalls that receive this hotfix will see an alert within the management interface, notifying them that the hotfix has been applied and whether or not the vulnerability has been exploited.ⁱⁱⁱ, & ^{iv}

Asnarök Malware

The Asnarök malware is a new threat that targets cybersecurity products, focused on gathering information about its targets by exploiting anti-malware programs' vulnerabilities.^v & ^{vi}

Patches and Mitigations

Sophos has released the software updates that address the CVE-2020-12271 vulnerability.

HPH entities are encouraged to:

- Keep the security products updated with the latest patches, and wherever possible, use automatic updates for such products to ensure immediate security from known threats.^{vii}
- Leverage a layered security architecture, by using a combination of multiple security products can help ensure better security across the technology stack.^{viii}
- Ensure the firewall administration interface (HTTPS admin service) or the user portal are not exposed on the WAN zone.



Health Sector Cybersecurity Coordination Center (HC3) Sector Alert

May 7, 2020

TLP: White

- Ensure unused interfaces are disabled to avoid their potential for unnoticed exploitation.
- Ensure firewalls that are manually configured to expose a firewall service (e.g. SSL VPN, SPX Portal) to the WAN zone does not share the same port as the admin or user portal.
- Scan for Indicators of Compromise (IOCs) associated with Asnarök malware provided in the Appendix.

Additional Resources

- Sophos, Fixing SQL injection vulnerability and malicious code execution in XG Firewall/SFOS, 5 May 2020, <https://community.sophos.com/kb/en-us/135412>
- UK National Cyber Security Center (NCSC) News, Sophos Vulnerability Statement, 28 April 2020, <https://www.ncsc.gov.uk/news/sophos-vulnerability-statement>
- Rapid7, CVE-2020-12271: Sophos XG Firewall Pre-Auth SQL Injection Vulnerability Remediation Guidance and Exposure Overview, 27 April 2020, <https://blog.rapid7.com/2020/04/27/cve-2020-12271-sophos-xg-firewall-pre-auth-sql-injection-vulnerability-remediation-guidance-and-exposure-overview/>
- National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD), CVE-2020-12271 Detail, 27 April 2020, <https://nvd.nist.gov/vuln/detail/CVE-2020-12271>

Indicators of Compromise (IOCs) Associated with Asnarökix

TLP:WHITE

Indicator type	Indicator
FileHash-SHA256	a226c6a641291ef2916118b048d508554afe0966974c5ca241619e8a375b8c6b
FileHash-SHA256	8e9965c2bb0964fde7c1aa0e8b5d74158e37443d857fc227c1883aa74858e985
FileHash-SHA256	4de3258ebba1ef3638642a011020a004b4cd4dbe8cd42613e24edf37e6cf9d71
FileHash-SHA256	31e43ecd203860ba208c668a0e881a260ceb24cb1025262d42e03209aed77fe4
FileHash-SHA256	736da16da96222d3dfbb864376cafd58239344b536c75841805c661f220072e5
FileHash-SHA256	9650563aa660ccbfd91c0efc2318cf98bfe9092b4a2abcd98c7fc44aad265fda
URL	https://sophosfirewallupdate.com/sp/sophos.dat
URL	https://sophosfirewallupdate.com/sp/lp
URL	https://sophosfirewallupdate.com/bk
URL	https://sophosfirewallupdate.com/sp/ae.sh
URL	https://ragnarokfromasgard.com/sp/patch.sh
URL	https://sophosfirewallupdate.com/in_exit
URL	http://filedownloaderservers.com/bkin
URL	https://sophosfirewallupdate.com/sp/Install.sh
URL	https://sophosfirewallupdate.com/sp/p.sh
URL	http://sophosfirewallupdate.com/sh_guard/lc
URL	http://sophosfirewallupdate.com/bkin
URL	https://sophosfirewallupdate.com/sp/lpin
domain	updatefilesservercross.com
domain	sophosfirewallupdate.com
domain	filedownloaderservers.com

TLP: WHITE

ID#202005061300, Pg. 4 of 4

HC3@HHS.GOV



Indicator type	Indicator
domain	sophotraining.org
domain	ragnarokfromasgard.com
domain	sophosproductupdate.com
domain	filedownloaderserver.com
domain	sophoswarehouse.com
domain	sophosenterprisecenter.com
domain	filedownloaderserverx.com

Figure 1. The indicators of compromise (IOCs) provided in the table above are classified TLP:WHITE. Source: AlienVault

Firewall Attack Stages and Artifacts

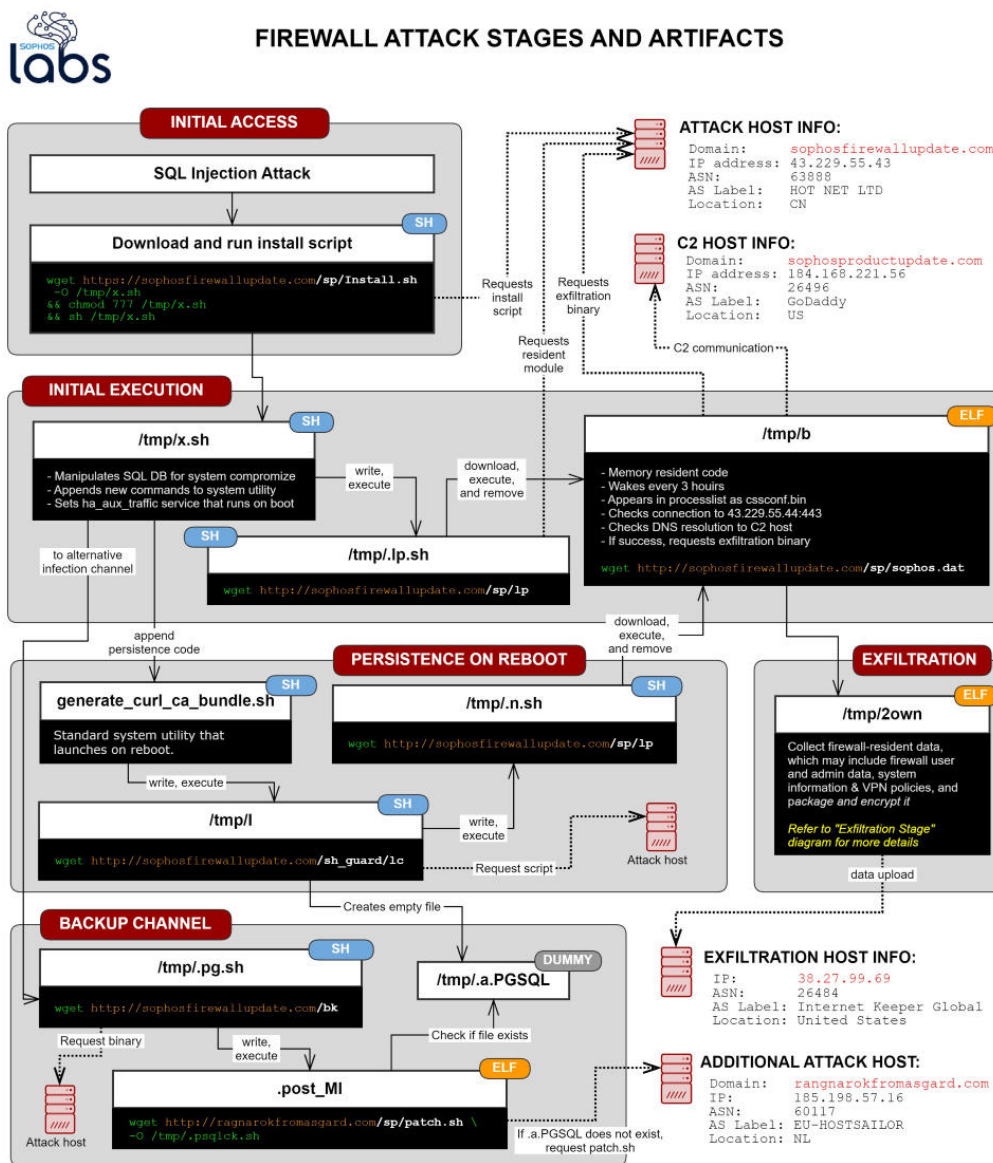


Figure 2. Firewall attack stages diagram with technical details. Source: Sophos.

TLP: WHITE

ID#202005061300, Pg. 4 of 4

HC3@HHS.GOV



References

- i <https://community.sophos.com/kb/en-us/135412>
- ii <https://www.tenable.com/blog/cve-2020-12271-zero-day-sql-injection-vulnerability-in-sophos-xg-firewall-exploited-in-the-wild>
- iii <https://cyware.com/news/asnarok-malware-dents-a-hole-in-sophos-xg-firewalls-13571dbe>
- iv <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12271>
- v <https://www.enigmasoftware.com/asnarok-removal/>
- vi <https://news.sophos.com/en-us/2020/04/26/asnarok/>
- vii <https://cyware.com/news/asnarok-malware-dents-a-hole-in-sophos-xg-firewalls-13571dbe>
- viii <https://cyware.com/news/asnarok-malware-dents-a-hole-in-sophos-xg-firewalls-13571dbe>
- ix <https://otx.alienvault.com/pulse/5ea6fc710b1e517cd25a7302>