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. 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.

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.

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.
- Leverage a layered security architecture, by using a combination of multiple security products can help ensure better security across the technology stack.
- Ensure the firewall administration interface (HTTPS admin service) or the user portal are not exposed on the WAN zone.
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**


**Indicators of Compromise (IOCs) Associated with Asnarökix**

<table>
<thead>
<tr>
<th>Indicator type</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileHash-SHA256</td>
<td>a226c6a641291ef2916118b048d508554afe0966974c5ca241619e8a375b8c6b</td>
</tr>
<tr>
<td>FileHash-SHA256</td>
<td>8e9965c2bb0964fde7c1aa0e8b5d74158e37443d857fc227c1883a74858e985</td>
</tr>
<tr>
<td>FileHash-SHA256</td>
<td>4de3258ebba1ef3638642a011020a004b4cd4dbe8cd42613e24edf37e6cf9d71</td>
</tr>
<tr>
<td>FileHash-SHA256</td>
<td>31e43ecd203860bxa208cs668a0e881a260cecb24cb1025262d42e03209aed77fe4</td>
</tr>
<tr>
<td>FileHash-SHA256</td>
<td>736da16a96222d3dfbb864376c4f58239344b536c75841805c661f220072e5</td>
</tr>
<tr>
<td>FileHash-SHA256</td>
<td>9650563aa660ccbfd91c0efc2318cf98bfe909b2a42abcd98c7fc44aad265fda</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://sophosfirewallupdate.com/sp/sophos.dat">https://sophosfirewallupdate.com/sp/sophos.dat</a></td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://sophosfirewallupdate.com/sp/lp">https://sophosfirewallupdate.com/sp/lp</a></td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://sophosfirewallupdate.com/bk">https://sophosfirewallupdate.com/bk</a></td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://sophosfirewallupdate.com/sp/ae.sh">https://sophosfirewallupdate.com/sp/ae.sh</a></td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://ragnarokfromasgard.com/sp/patch.sh">https://ragnarokfromasgard.com/sp/patch.sh</a></td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://sophosfirewallupdate.com/sp/install.sh">https://sophosfirewallupdate.com/sp/install.sh</a></td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://sophosfirewallupdate.com/sp/p.sh">https://sophosfirewallupdate.com/sp/p.sh</a></td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://sophosfirewallupdate.com/sh_guard/lc">http://sophosfirewallupdate.com/sh_guard/lc</a></td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://sophosfirewallupdate.com/bkin">http://sophosfirewallupdate.com/bkin</a></td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://sophosfirewallupdate.com/sp/lpin">https://sophosfirewallupdate.com/sp/lpin</a></td>
</tr>
<tr>
<td>domain</td>
<td>updatefileservercross.com</td>
</tr>
<tr>
<td>domain</td>
<td>sophosfirewallupdate.com</td>
</tr>
<tr>
<td>domain</td>
<td>filedownloaderservers.com</td>
</tr>
</tbody>
</table>
## Indicator type

<table>
<thead>
<tr>
<th>Indicator type</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>sophostraining.org</td>
</tr>
<tr>
<td>domain</td>
<td>ragnarokfromasgard.com</td>
</tr>
<tr>
<td>domain</td>
<td>sophosproductupdate.com</td>
</tr>
<tr>
<td>domain</td>
<td>filedownloaderserver.com</td>
</tr>
<tr>
<td>domain</td>
<td>sophoswarehouse.com</td>
</tr>
<tr>
<td>domain</td>
<td>sophosenterprisecenter.com</td>
</tr>
<tr>
<td>domain</td>
<td>filedownloaderserverx.com</td>
</tr>
</tbody>
</table>

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.

**INITIAL ACCESS**

SQL Injection Attack

- Download and run install script

**INITIAL EXECUTION**

- Exploits SQL DB for system compromise
- Assembles new commands to system utility
- Sets for _alt_traffic service that runs on boot

**PERSISTENCE ON REBOOT**

- Standard system utility that launches on reboot

**EXFILTRATION**

- Collects firewall resident data, which may include firewall user and alert info
- Number of _alt_traffic services

**EXFILTRATION HOST INFO:**
- IP: 58.35.95.65
- AS Label: Internet Keeper Global
- Location: United States

**ADDITIONAL ATTACK HOST:**
- Domain: sophoswarehouse.com
- IP: 10.10.57.16
- AS Label: EC-N0079A120
- Location: NL

**DEFENSE IN DEPTH**

- Requires host firewall binary
- Requires resident binary
- Requires resident module
- C2 communication
- C2 Host info

**ATTACK HOST INFO:**
- Domain: sophosproductupdate.com
- IP address: 43.229.55.43
- AS Label: CHEF NET LTD
- Location: CH

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

i https://community.sophos.com/kb/en-us/135412
iv https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12271
v https://www.enigmasoftware.com/asnarok-removal/
ix https://otx.alienvault.com/pulse/5ea6fc710b1e517cd25a7302