# CVE Detail – CVE-2020-12271

A SQL injection issue was found in SFOS 17.0, 17.1, 17.5, and 18.0 before 2020-04-25 on Sophos XG Firewall devices, as exploited in the wild in April 2020. This affected devices configured with either the administration (HTTPS) service or the User Portal exposed on the WAN zone. A successful attack may have caused remote code execution that exfiltrated usernames and hashed passwords for the local device admin(s), portal admins, and user accounts used for remote access (but not external Active Directory or LDAP passwords)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.99198

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

## CAPEC(s)

* CAPEC-108: Command Line Execution through SQL Injection
* CAPEC-109: Object Relational Mapping Injection
* CAPEC-110: SQL Injection through SOAP Parameter Tampering
* CAPEC-470: Expanding Control over the Operating System from the Database
* CAPEC-66: SQL Injection
* CAPEC-7: Blind SQL Injection

## Affected Products

* cpe:2.3:o:sophos:sfos:17.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:sophos:sfos:17.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:sophos:sfos:17.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:sophos:sfos:18.0:\*:\*:\*:\*:\*:\*:\*