NVD DB Update

CVE-2020-12271 - Score: 9.8

Components:

sophos sfos 17.1
sophos sfos 18.0
sophos sfos 17.0
sophos sfos 17.5
sophos xg firewall -

Description:

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)

Main problems:

89 "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')"

https://cybersword.tech
ph1sher
www.linkedin.com/in/cybersword-tech
@davidwowa