Sophos XG-firewalls doelwit van zeroday-aanval

XG-firewalls van Sophos zijn afgelopen week het doelwit van een zeroday-aanval geweest, zo heeft het securitybedrijf zelf bekendgemaakt. Via een tot dan toe onbekende SQL-injection kwetsbaarheid wisten aanvallers toegang tot Sophos XG-firewalls te krijgen en gegevens over gebruikers te downloaden.

Het gaat dan om gebruikersnamen en gehashte wachtwoorden voor de lokale beheerder(s), portalbeheerder(s) en gebruikersaccounts voor remote toegang. Sophos stelt dat erop dit moment geen aanwijzingen zijn dat bij de aanvallen er toegang is verkregen tot het lokale netwerk achter de firewall. De eerste aanvallen vonden volgens het securitybedrijf op 22 april plaats. Gisteren werd er onder klanten die automatisch updaten hebben ingeschakeld een hotfix uitgerold die de kwetsbaarheid verhelp en "overblijfselen" van de aanval verwijdert.

Wanneer de firewall is gecompromitteerd krijgen beheerders in hun interface een waarschuwing te zien. **Sophos adviseert** eigenaren van een gecompromitteerde firewall om de wachtwoorden voor beheerders en gebruikers te resetten en het apparaat te herstarten