Sophos

Produktet Sophos XG Firewall, viktime të një sulmi zero-day

Firma e sigurisë Sophos dhe klientët e saj u sulmuan kur një dobësi më parë e panjohur "injeksion SQL" u shfrytëzua në njësitë fizike dhe virtuale të Firewall XG të kompanisë.

Sulmi u raportua së pari më 22 Prill kur u zbulua një vlerë e dyshimtë e dukshme në ndërfaqen e menaxhimit të firewallit. Sulmi krijoi një situatë të ekzekutimit të kodit në distancë, e cila u mundësoi sulmuesve të fitojnë akses në pajisjet e ekspozuara XG me qëllim të shfarosjes së të dhënave rezidente të XG Firewall. Kjo përfshinte të gjitha emrat e përdoruesve lokalë dhe fjalëkalimet e fshehura të çdo llogarie të përdoruesit lokal.

Sulmi afektoi sistemet e konfiguruara me ndërfaqen e administrimit (shërbimin e administratorit HTTPS) ose me portalin e përdoruesit të ekspozuar në zonën WAN. Përveç kësaj, firewallet e konfiguruar manualisht për të ekspozuar një shërbim (p.sh. SSL VPN) në zonën WAN që ndajnë të njëjtën porte me administratorin ose Portalin e Përdoruesit gjithashtu u prekën.

Reagimi fillestar i Sophos ishte të përcaktonte përbërësit e sulmit dhe të aplikonte një hotfix që eliminoi kërcënimin për të gjitha versionet e mbështetura XG Firewall / SFOS. Kompania njoftoi klientët e saj për kërcënimin, nëse sistemi i tyre ishte i përfshirë apo jo në sulm dhe aplikimin e hotfix-it përmes një mesazhi pop-up në ndërfaqen e menaxhimit XG.

Shfrytëzimi i kësaj dobësie rezultoi që sulmuesi të ishte në gjendje të fuste një komandë në një tabelë të dhënash. Kjo komandë fillestare e injektuar shkaktoi qe pajisja e prekur të shkarkoje një skript shell Linux të quajtur Install.sh nga një server i largët në sofosfirewallupdate.com domain [me qëllim të keq].