

ارتقای Firmware در فایروال‌های

Sophos XG

و ترمیم آسیب‌پذیری SQL Injection

طبق اعلام شرکت سوفوس، اخیراً یک ضعف امنیتی از نوع SQL Injection در فایروال‌های سری XG سوفوس کشف شده که می‌تواند موجب دسترسی غیرمجاز به فایروال گردد.

سوءاستفاده از این ضعف امنیتی صرفاً در صورتی ممکن است که سرویس‌های User Portal یا HTTPS برای WAN Zone باشد. فایروال‌هایی که این دو سرویس آنها برای WAN Zone بسته باشد در مقابل دسترسی غیر مجاز ایمن می‌باشند. بنابراین در گام اول برای جلوگیری از هرگونه مشکل امنیتی توصیه می‌شود که دو سرویس فوق برای WAN Zone بسته شوند.

شکل زیر محل انجام این کار در صفحه Administration/Device Access از تنظیمات فایروال را نشان می‌دهد. تیک سرویس‌های HTTPS و User Portal را در ردیف WAN بردارید و Apply کنید.


Zone	Admin services		Authentication services				Network services			Other services						
	HTTPS	SSH	AD SSO	Captive portal *	Radius SSO	Client Authentication	Chromebook SSO	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web proxy	User Portal	Dynamic Routing	SMTP Relay	SNMP
LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WIFI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Turning off access to captive portal stops user notifications from appearing. Example: Web filter and Sandstorm notification pages

شرکت سوفوس برای رفع ضعف امنیتی فوق یک نسخه جدید Firmware منتشر کرده است که می‌توانید از آدرس زیر آن را دریافت و نصب کنید.

http://s.sgcompute.co/xg/hw/patch/HW-17.5.12_MR-12.SF300-664.gpg

مراحل نصب نسخه جدید Firmware به شرح زیر می‌باشد.

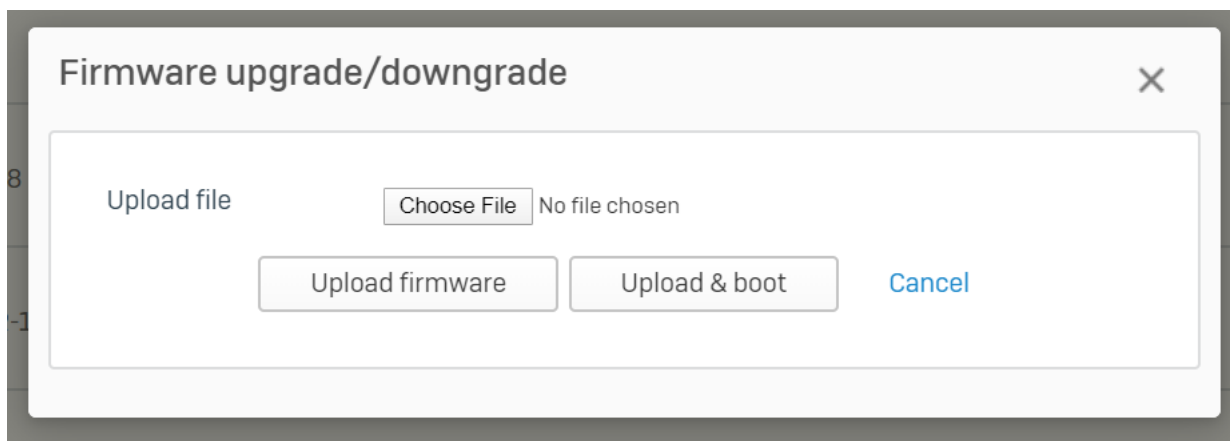
1- طبق شکل زیر به صفحه Backup & Firmware/Firmware مراجعه کرده و بر روی دکمه  (Upload) کلیک کنید.


Version	Active	Manage
SFOS 17.5.8 MR-8	<input checked="" type="checkbox"/>	<input type="button" value="Upload"/> <input type="button" value="Refresh"/> <input type="button" value="Settings"/>
SFOS 17.5.11 MR-11	<input type="checkbox"/>	<input type="button" value="Refresh"/> <input type="button" value="Settings"/>

Latest available firmware

Firmware version	Type	Actions
No records found		

- ۲- فایل Firmware جدید را که از آدرس فوق دانلود کرده‌اید انتخاب و بارگذاری کنید.
- ۳- در پنجره‌ای که برای انتخاب فایل Firmware باز می‌شود دو گزینه Upload firmware و Upload & boot وجود دارد. نصب Firmware جدید همراه با راه‌اندازی مجدد (Reboot) فایروال است. اگر می‌خواهید در همین لحظه نصب و راه‌اندازی مجدد انجام شود دکمه Upload & reboot را بزنید. اگر می‌خواهید بعداً در زمان مناسبی فایروال را راه‌اندازی مجدد کنید، دکمه Upload firmware را بزنید. در این حالت فایل Firmware روی سیستم بارگذاری می‌شود اما نصب و راه‌اندازی مجدد را می‌توانید بعداً در زمان مناسب انجام دهید.



- در صورتی که دکمه upload firmware را انتخاب کرده‌اید هر زمان که بخواهید Firmware جدید نصب شود کافی است که دکمه  را در سطر مربوط به Firmware جدید بزنید.
- شرکت سوفوس توصیه می‌کند که برای امنیت بیشتر رمز ورود admin فایروال را نیز تغییر دهید.

مرکز آموزش

events.shabakeh.net

اتاق خبر

newsroom.shabakeh.net

تارنمای شرکت

www.shabakeh.net

خدمات پس از فروش و پشتیبانی

my.shabakeh.net

درباره ما

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تاسیس شد. این شرکت یکی از با سابقه‌ترین شرکت‌های فعال در حوزه امنیت فناوری اطلاعات است. با بیش از ۲۸ سال تجربه موفق در عرضه محصولات و خدمات امنیت شبکه، شرکت شبکه گستر افتخار خدمات‌دهی به هزاران شرکت و سازمان در بخش‌های مختلف کشور را دارد و مجری بزرگترین پروژه‌های نصب و نگهداری نرم‌افزارهای ضدبدافزار و سخت‌افزارهای دیواره آتش در کشور بوده است.

تهران خیابان شهید دستگردی (ظفر) شماره ۲۷۳

تلفن / دورنگار ۰۲۱ - ۴۲۰۵۲

www.shabakeh.net

info@shabakeh.net

شبکه گستر

امنیت شما | وظیفه ما