DIGITEMIS
CYBERSECURITY & PRIVACY

StormShield – SNS – Versions 3.0.0 à 4.0.1

Redirection Arbitraire

Bulletin de sécurité
20/02/2020

Romain KOSZYK (_ACKNAK_)

Description

Le portail captif du VPN SSL StormShield est vulnérable à une redirection arbitraire.

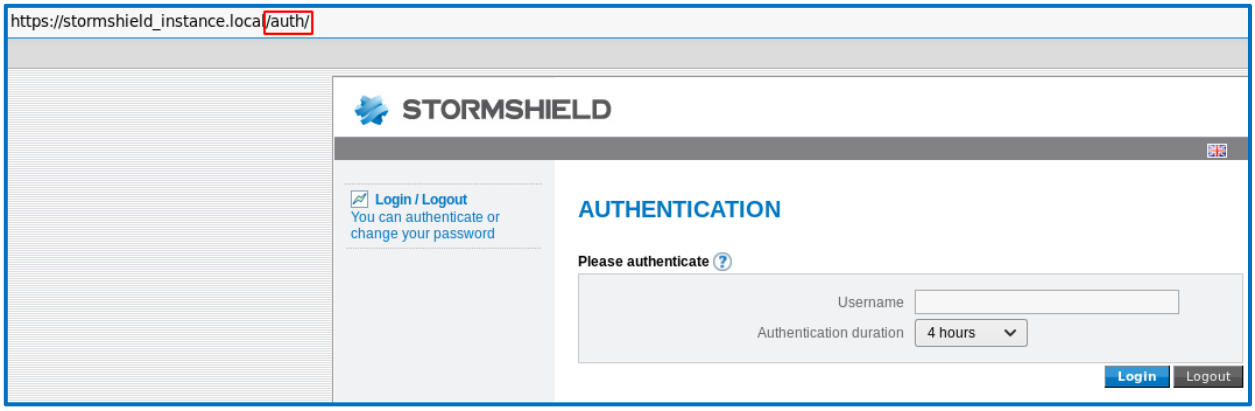

Figure 1 – Portail captif d'une instance VPN SSL de StormShield

Cela permet à un attaquant de rediriger une victime vers un site malveillant. La réussite d'une telle attaque implique donc une campagne de phishing. Les utilisateurs pourraient donc être redirigés vers une mire d'authentification StormShield malveillante. Le paramètre vulnerable est le suivant :

*https://stormshield_instance.local/auth/lang.html?l=en&**rurl=%2f%2fgoogle.com***

Le paramètre "*rurl*" est vulnérable bien que des protections contre ce type d'attaque soient déjà en place. Ces protections peuvent être contournées en utilisant **//site.com** plutôt que *protocole://site.com* ou encore *protocole:site.com*.

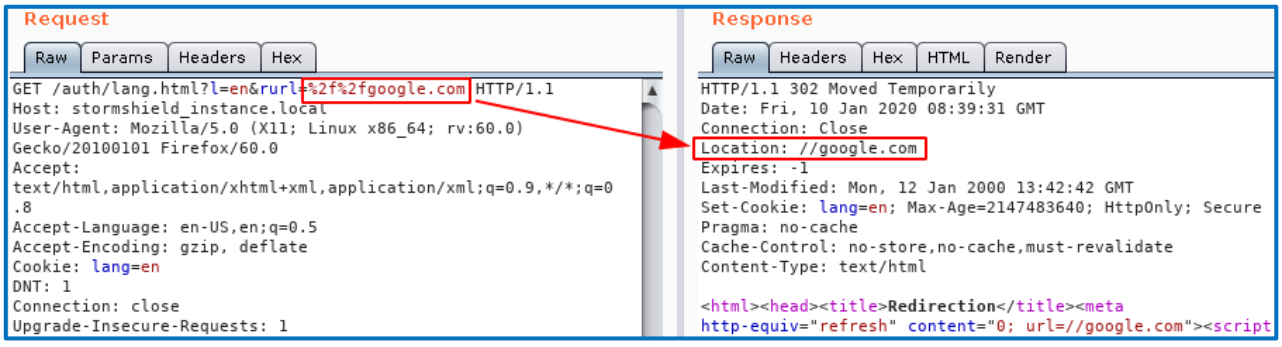

Figure 2 – Redirection arbitraire via l'utilisation de //site.com

Un attaquant pourrait envoyer un mail à l'administrateur avec le lien suivant :

*https://stormshield_instance.local/auth/lang.html?l=en&**rurl=%2f%2fstormshield_attacker_instance.local/admin/admin.html***

L'administrateur serait alors redirigé vers le site de phishing de l'attaquant.

Impacts & Risques

Les administrateurs et utilisateurs pourraient être compromis via une attaque de phishing en abusant de la redirection arbitraire sur les SNS.

Les versions SNS 3.0.0 à 4.0.1 sont affectées par cette vulnérabilité.

Recommendation

Une mise à jour vers les versions 3.7.11, 3.10.1 et 4.0.2 permettra de corriger la vulnérabilité.

Le bulletin de sécurité de StormShield est disponible à l'URL suivante:

https://advisories.stormshield.eu/2020-001/

Timeline

2020-01-09: Découverte de la vulnérabilité
2020-01-17: Envoi des details techniques à l'équipe de sécurité SNS de StormShield
2020-01-24: L'équipe de sécurité de StormShield a confirmé la vulnérabilité
2020-01-29: Mitre a affecté le numéro CVE-2020-8430 à cette vulnérabilité
2020-02-19: StormShield a publié un bulletin de sécurité avec les recommendations associées

Références

CVE: (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8430)
StormShield: (https://advisories.stormshield.eu/2020-001/)

Contact

romain.koszyk@digitemis.com