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.


**CVE:** [http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6412](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

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


**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.

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.
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

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.