Sophos Web Appliance – Block & Unblock IPs Remote Command Injection

Security Advisory	AE-Advisory 17-03	**Criticality**	Critical	
Advisory Released On	31 January 2017			

Impact

Compromise of the appliance's Linux subsystem

Remote command injection

Solution

Adhere the advices written under the solution section.

Affected Platforms

- Sophos Web Appliance below version 4.3.1.3 (confirmed in 4.2.1.3)

CVE Reference

- CVE-2016-9553

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about two new vulnerabilities in the Sophos Web Appliance. The two vulnerabilities include attackers being able to use Remote Command Injection against vulnerable appliances. The vulnerabilities have now been patched in the January 2017 4.3.1 release of the appliance line. Further information is explained in the Threat Details section below.

Threat Details

The Sophos Web Appliance (version 4.2.1.3) is vulnerable to two Remote Command Injection vulnerabilities in its web administrative interface. The vulnerabilities occur in the "MgrReport.php (/controllers/MgrReport.php)" component that is responsible for blocking and unblocking IP addresses that can access the appliance.

The appliance is not able to properly escape the information submitted in the variables 'unblockip' and 'blockip' before calling out the "shell_exec()" function. From the name of the function, we can tell that it is responsible for executing systems commands into the appliance.

The page that contains these two vulnerabilities (/controllers/MgrReport.php) is accessed by several of the machine's built-in commands in the administrative interface. The pages that call to the vulnerable page are:

- 'report'
- 'trend_volume'
- trend_suspect'
- 'top_app_ctrl'
- perf_latency'
- 'perf_throughput'
- 'users_browse_summary'
- 'traf_sites'
- 'traf_blocked'
- 'traf_users'
- 'users_virus_downloaders'
- 'users_pua_downloaders'
- 'users_highrisk'
- 'users_policy_violators'
- 'users_top_users_by_browse_time'
- 'users_quota'
- 'users_browse_time_by_user'
- 'users_top_users_by_category'
- 'users_site_visits_by_user'
- 'users_category_visits_by_user'
- 'users_monitored_search_queries'
- 'users_app_ctrl'
- 'traf_category'
- 'traf_download'
- 'warned_sites'

Once an attacker is able to exploit this vulnerability, they are granted shell access to the victim machine.

Solution

This vulnerability has now been patched in the January 2017 4.3.1 release of the appliance line. Please refer to your network administrator for applying the latest patches to your Sophos Web Appliance device(s) to prevent being a possible victim of this vulnerability.

For more information regarding the patch release, please visit the URL below:

http://swa.sophos.com/rn/swa/concepts/ReleaseNotes_4.3.1.html

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae