[R5] SecurityCenter 5.4.3 Fixes Multiple Vulnerabilities

Medium

← View more security advisories

Synopsis

SecurityCenter has recently been discovered to contain several vulnerabilities. Four issues in the SC code were discovered during internal testing by Barry Clark, and several third-party libraries were upgraded as part of our internal security process. Note that the library vulnerabilities were not fully diagnosed so SecurityCenter is possibly impacted. Tenable opted to upgrade the libraries as it was more efficient than diagnosing each issue. Details of the issues are below, with VDB IDs and/or internal IDs for your tracking pleasure. Note that not all library vulnerabilities have a CVE assignment:

- PHP ext/phar/phar.c phar_parse_pharfile() Function Phar Archive Handling Out-of-bounds Read DoS
- PHP ext/exif/exif.c exif_convert_any_to_int() Function TIFF / JPEG Image Tag Handling Floating Pointer Exception Remote DoS (CVE-2016-10158)
- PHP ext/standard/var_unserializer.c finish_nested_data() Function Unserialized Data Handling Out-of-bounds Read Remote Weakness (CVE-2016-10161)
- PHP ext/phar/phar.c phar_parse_pharfile() Function Phar Archive Handling Off-by-one Remote Buffer Overflow DoS (CVE-2016-10160)
- PHP ext/phar/phar.c phar_parse_pharfile() Function Phar Archive Handling Integer Overflow DoS (CVE-2016-10159)
- GD Graphics Library (LibGD) gd_gd2.c gdImageCreateFromGd2Ctx() Function Insufficient Image Data Handling DoS (CVE-2016-10167)

- OpenSSL crypto/bn/asm/x86_64-mont.pl Montgomery Multiplication Incorrect Results Weakness (CVE-2016-7055)
- Apache HTTP Server User-Agent Whitespace Pattern Handling Cache Pollution Response Confusion Cross-session Information Disclosure (CVE-2016-8743)
- Apache HTTP Server modules/aaa/mod_auth_digest.c Client Entry Allocation Shared Memory Space Exhaustion Remote DoS (CVE-2016-2161)
- Apache HTTP Server Session Data / Cookie Padding Oracle Attack Information Disclosure Weakness (CVE-2016-0736)
- Apache HTTP Server mod_http2 HTTP/2 CONTINUATION Frame Handling Memory Exhaustion Remote DoS (CVE-2016-8740)
- Apache HTTP Server Proxy Header Injection HTTP_PROXY Environment Variable Overwrite Remote Proxy Manipulation (CVE-2016-5387 / CVE-2016-1000104 / CVE-2016-1000102)
- libcurl lib/rand.c randit() Function Uninitialized Random Value Weak Cryptographic Operations (CVE-2016-9594)
- Authenticated Stored XSS (Internal ID 31620)
- Authenticated Stored XSS (Internal ID 31619)
- Authenticated Stored XSS (Internal ID 31498)
- Authenticated Stored XSS (Internal ID 31430)

Please note that Tenable strongly recommends that SecurityCenter be installed on a subnet that is not Internet addressable.

Solution

Tenable has released SecurityCenter 5.4.3 to address these issues. The new version can be obtained from the Tenable Support Portal (https://support.tenable.com/support-center/index.php?x=&mod_id=160).

Additionally, patches have been created to address these issues for Security Center 5.0.2 through 5.4.2. The patches and associated checksums can be found at http://static.tenable.com/prod_docs/upgrade_security_center.html.

Tenable has released version 4.5.0 of the Appliance that resolves this issue. Users are strongly encouraged to use the online updating functionality or download the new version to upgrade.

https://www.openssl.org/news/secadv/20160128.txt

This page contains information regarding security vulnerabilities that may impact Tenable's products. This may include issues specific to our software, or due to the use of third-party libraries within our software. Tenable strongly encourages users to ensure that they upgrade or apply relevant patches in a timely manner.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: CVE-2016-0736
CVE-2016-2161
CVE-2016-5387
CVE-2016-7055
CVE-2016-8740
CVE-2016-8743
CVE-2016-9594
CVE-2016-10158
CVE-2016-10160
CVE-2016-10161
CVE-2016-10159
CVE-2016-10167
CVE-2016-1000102
CVE-2016-1000104
CVE-2017-3731
CVE-2017-3732
Tenable Advisory ID: TNS-2017-04
Risk Factor: Medium
Credit:
Barry Clark [Tenable Network Security]

Affected Products

SecurityCenter: 5.0.2, 5.1.0, 5.2.0, 5.3.1, 5.3.2, 5.4.0, 5.4.1, 5.4.2
Tenable Appliance: 4.4.0

Disclosure Timeline

2017-02-09 - SecurityCenter 5.4.3 Released

Advisory Timeline

2017-02-14 - [R1] Initial Release
2017-02-17 - [R2] Additional SC versions impacted, patch information
2017-02-28 - [R3] Adjust CVSS for worst-case scenario (AV:A -> AV:N)
2017-03-07 - [R4] Added Tenable Appliance info
2017-03-08 - [R5] Fixed typo in SC versions (5.4.2 twice, should be 5.4.1/5.4.2)

>

View all ›

Featured solutions

Active Directory

Building management systems

Cloud security posture management

Compliance

Exposure management

Banks and financial services

Healthcare

Hybrid cloud security

IT/OT

Ransomware

State / Local / Education

US federal

Vulnerability management

Zero trust

View all ›

Customer resources

Resource library

Exposure management resources

Community & support

Customer education

Tenable Research

Documentation

Cybersecurity guide