Skybox Product Security Advisory

ADVISORY ID: SKYBOX-2017-002

PUBLISH DATE: SEPTEMBER 25, 2017

ARTICLE VERSION: 1.0

Notice of Vulnerabilities in Skybox Manager Client Application

Background:

This advisory provides information about four vulnerabilities found in the Skybox Manager Client Application. The CVSS scores range from 2.5 to 7. All require local access to the affected machine.

Privilege Elevation Vulnerability Upon Authentication

Skybox Manager Client Application versions 8.5.500 and earlier are susceptible to an elevation of privileges vulnerability while authenticating a valid user in a debugger-pause state. The vulnerability can only be exploited by a local authenticated attacker.

CVE ID: CVE-2017-14773
CVSS Score: 7.0
CVSS Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Arbitrary File Upload Vulnerability

Skybox Manager Client Application versions 8.5.500 and earlier are susceptible to an arbitrary file upload vulnerability due to insufficient input validation of user-supplied files path when uploading files via the application. During a debugger-pause state, a local authenticated attacker can upload an arbitrary file and overwrite existing files within the scope of the affected application. The vulnerability can only be exploited by a local authenticated attacker.

CVE ID: CVE-2017-14771
CVSS Base score: 6.0
CVSS Base Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:H

Information Disclosure Vulnerability via Username Enumeration

Skybox Manager Client Application is prone to information disclosure via a username enumeration attack. A local unauthenticated attacker could exploit the flaw to obtain valid usernames, by analyzing error messages upon valid and invalid account login attempts.

CVE ID: CVE-2017-14772
CVSS Base Score: 4.0
CVSS Base Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Information Disclosure of Password Hash

Skybox Manager Client Application versions 8.5.500 and earlier are susceptible to an information disclosure vulnerability of user password hashes. A local authenticated attacker can access the password hashes in a debugger-pause state during the authentication process. The vulnerability can only be exploited by a local authenticated attacker.

CVE ID: CVE-2017-14770
CVSS Base Score: 2.5
CVSS Base Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N

Affected platforms and Versions

The following products are affected:

- Skybox Manager Client Application versions 8.5.500 and earlier are susceptible to CVE-2017-14770, CVE-2017-14771, CVE-2017-14773.
- At this time, all versions are affected by CVE-2017-14772.

How to check your Skybox Version

1. Using Skybox Manager Client Application:
   a. Login to the Skybox Manager client application
   b. Supply login credentials
   c. On the top toolbar, select 'Help' → 'About Skybox', and check for 'version' entry
   d. If the Version is **8.5.500 or earlier**, then this system is vulnerable and updating to version 8.5.501 or later is recommended.

Remediation Instructions

For CVE IDs: CVE-2017-14773, CVE ID: CVE-2017-14771, CVE ID: CVE-2017-14770: Update your Skybox platform to version 8.5.501 or later. Update instructions can be found in the Skybox Administration Guide.

For CVE-2017-14772: At the present time there is no remediation available.

Support

For additional information and technical support resources, contact Skybox Security at support@skyboxsecurity.com