Plex Media Server Local Privilege Escalation (Windows)

High

← View More Research Advisories

Synopsis

The Plex Update Service ("Plex Update Service.exe") contains a flaw that allows a local attacker to execute arbitrary Python code with SYSTEM privileges. The service exposes functionality over an ALPC port that can be invoked by a local, unauthenticated attacker.

The service is defined as such:

```
[
uuid(631c7d9c-1797-42f9-8e96-367a9ee58887),
version(1.0),
]
interface DefaultIfName
{

void Proc0(
        [in][string] wchar_t* arg_1);

long Proc1(
        [in][string] wchar_t* arg_1);

long Proc2(
        [in][string] wchar_t* arg_1,
        [out]long *arg_2);
}
```

Specifically, Proc2 will execute a given executable if it is signed by Plex, even if it is not a legitimate update file. PlexScriptHost.exe (a Python interpreter) happens to be signed by Plex, and if a file named 'sitecustomize.py' is located in the current working directory, it will be executed when PlexScriptHost is launched. This is expected behavior for Python interpreters, and it can be abused to execute arbitrary code contained in sitecustomize.py.

Proof of Concept

https://github.com/tenable/poc/tree/master/plex/plex_media_server/tra_2020_25
Run the PoC and notice that the process is launched as SYSTEM. You will need to inspect the task list.

Launch RpcClient.exe to execute a command of your choosing, or by default execute the Windows Calculator. Below will add a new user.

```
> RpcClient.exe "net user /add scooby"
```

Below is a log entry in Plex Update Service.log showing a successful exploitation attempt.

```
Mar 31, 2020 14:05:05.324 [4796] DEBUG - Install() from UpdateInterface: C:\Users\lowpriv\Documents\RpcClient\RpcClient\Release\PlexScriptHost.exe
Mar 31, 2020 14:05:05.324 [4796] DEBUG - CheckBundle() from UpdateInterface: C:\Users\lowpriv\Documents\RpcClient\RpcClient\Release\PlexScriptHost.exe
Mar 31, 2020 14:05:05.324 [4796] DEBUG - Checking Certificate of installer: C:\Users\lowpriv\Documents\RpcClient\RpcClient\Release\PlexScriptHost.exe
Mar 31, 2020 14:05:05.324 [4796] DEBUG - Certificate integrity verified
Mar 31, 2020 14:05:05.324 [4796] DEBUG - HTTP requesting GET https://plex.tv/api/pmscert/profile
Mar 31, 2020 14:05:05.839 [4796] DEBUG - HTTP 200 response from GET https://plex.tv/api/pmscert/profile
Mar 31, 2020 14:05:05.839 [4796] DEBUG - Certificate identity verified
Mar 31, 2020 14:05:05.839 [4796] DEBUG - Create Process Success! Waiting for process to complete.
Mar 31, 2020 14:05:05.932 [4796] DEBUG - Installer exit code:  2 - The system cannot find the file specified.
```

Solution

Upgrade to 1.18.2 or newer. Additionally, Plex Media Server versions 1.19.1.2701 & 1.19.2.2702 (and newer) features additional hardening in the updater infrastructure to protect against future vulnerabilities

Additional References

https://forums.plex.tv/t/security-regarding-cve-2020-5740/579634

Disclosure Timeline

03/31/2020 - Tenable reports vulnerability
03/31/2020 - Plex is looking at the issue. They were able to download the PoC.
04/01/2020 - Tenable acknowledges.
04/03/2020 - Plex proposes a fix strategy. Also notifies me of bounty payout.
04/06/2020 - Tenable acknowledges fix strategy. Asks about anticipated patch release date.
04/07/2020 - Some back-and-forth on bounty specifics.
04/07/2020 - Plex hopes to release a patch before the end of the month. Nothing firm yet.
04/07/2020 - Tenable acknowleges.
04/07/2020 - More bounty specifics.
04/20/2020 - Plex sends a link to a beta update package. Asks if I will confirm the fix.
04/21/2020 - Tenable confirms that the package fixes the vulnerability. Exploit no longer works.

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

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

Risk Information

CVE ID: CVE-2020-5740
Tenable Advisory ID: TRA-2020-25
Credit: Chris Lyne

CVSSv2 Base / Temporal Score: 7.2 / 5.6
CVSSv2 Vector: (AV:L/AC:L/Au:N/C:C/I:C/A:C)
Affected Products: Plex Media Server (Windows) prior to 1.18.2
Risk Factor: High

Advisory Timeline

04/21/2020 - Advisory released
04/24/2020 - Updated fix version
04/27/2020 - Added reference to Plex forum post
04/30/2020 - Updating vuln version and solution

FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

Careers

Investors

Events

Media

tenable

Privacy Policy Legal 508 Compliance