Plex Media Server Weak CORS Policy

Medium

← View More Research Advisories

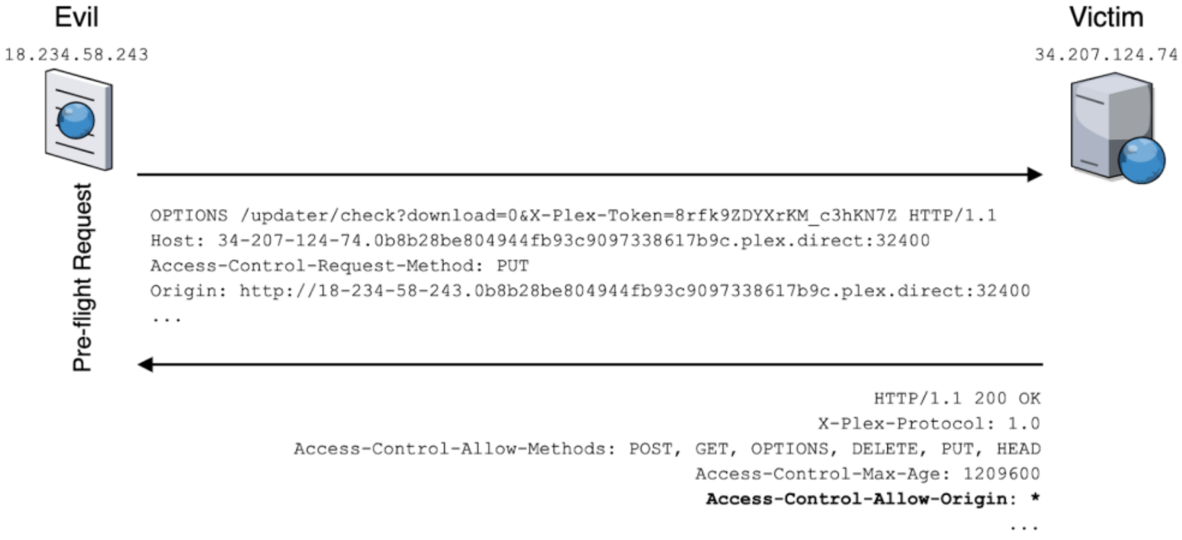
Synopsis

The Plex Media Server has a weak cross-origin resource sharing (CORS) policy. By default, an Access-Control-Allow-Origin header is returned by a media server with a value of '*', meaning any origin is allowed to send requests to the media server. A remote, unauthenticated attacker is able to exploit this to steal an X-Plex-Token and/or force a victim user to send requests to their own server without their knowledge. This would allow the attacker to, for example, access private media, change server settings, reboot media server services, etc.

This vulnerability would be exploited via a phishing attack, where a victim admin user would be tricked into logging into the attacker's Plex Media Server. The client-side code in the victim's browser, hosted by the attacker's media server, would then be able to access media server(s) that the victim administers. This scenario is shown in the PoC below.

Proof of Concept

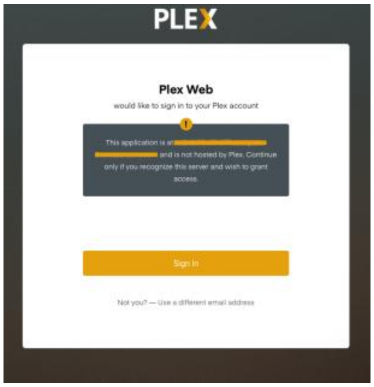
In the image below, a victim user hosts a Plex Media Server at 34.207.124.74, and an attacker hosts a media server at 18.234.58.243. The victim user just logged into the attacker's server, and the following preflight request/response was observed.



```
OPTIONS /updater/check?download=0&X-Plex-Token=8rfk9ZDYXrKM_c3hKN7Z HTTP/1.1
Host: 34-207-124-74.0b8b28be804944fb93c9097338617b9c.plex.direct:32400
Access-Control-Request-Method: PUT
Origin: http://18-234-58-243.0b8b28be804944fb93c9097338617b9c.plex.direct:32400
...
```

```
                                          HTTP/1.1 200 OK
                                    X-Plex-Protocol: 1.0
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT, HEAD
                            Access-Control-Max-Age: 1209600
                              Access-Control-Allow-Origin: *
                                                         ...
```

Note, the IP addresses in the video differ from the previous example.



Plex Web

would like to sign in to your Plex account

This application is at [redacted] and is not hosted by Plex. Continue only if you recognize this server and wish to grant access.

Not you? — Use a different email address

Disclosure Timeline

03/31/2020 - Tenable reports vulnerability to Plex.
03/31/2020 - Automated reply received
03/31/2020 - Plex thanks Tenable for another vulnerability submission
04/01/2020 - Tenable ACKs
04/10/2020 - Tenable follows up. Asks if they have any questions or comments about the report.
04/22/2020 - Plex indicates it's not an easy thing to fix. Asks for clarification on 90-day policy.
04/22/2020 - Tenable clarifies our policy.
05/01/2020 - Tenable asks for an update.
05/05/2020 - Plex is still discussing a solution. They hope to have a fix in place before the 90-day deadline.
05/12/2020 - Tenable thanks Plex for the update.
05/21/2020 - Tenable asks for an update.
05/26/2020 - Plex says the team is still working on it. They think we can make some mitigations before the deadline.
05/27/2020 - Tenable says thanks.
06/08/2020 - Tenable notifies Plex of intent to publish blogs. Also asks for an update.
06/09/2020 - Plex gives us some info about the intended patch. Also says they would be happy to review the blogs.
06/09/2020 - Tenable acknowledges. Asks for anticipated release date. Shares blog drafts.
06/10/2020 - Plex doesn't have an ETA on the fix, but will update us. Asks us to change some wording.
06/11/2020 - Tenable thanks for the update. Asks for clarification on wording.
06/12/2020 - Plex clarifies.
06/15/2020 - Plex notifies Tenable that they deployed a mitigation.
06/15/2020 - Tenable asks if there is any specific mitigation guidance.
06/15/2020 - Plex says no. Changes are server side.

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.

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-2020-5742
Tenable Advisory ID: TRA-2020-35
Credit: Chris Lyne

CVSSv2 Base / Temporal Score: 6.8 / 5.3
CVSSv2 Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
Affected Products: Plex Media Server prior to June 15, 2020
Risk Factor: Medium

Advisory Timeline

06/15/2020 - Advisory published.

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 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

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media

Privacy Policy Legal 508 Compliance