

12

## Redirect on authorization allows account compromise

Share:



State

Resolved (Closed)

Disclosed

November 6, 2018 9:53pm +0100

Reported To

TTS Bug Bounty

Asset

\*.login.gov  
(Domain)


Weakness

Improper Authentication - Generic

Severity

Critical (9 ~ 10)

Participants



Visibility

Disclosed (Limited)

Collapse

### SUMMARY BY TTS BUG BOUNTY



Login.gov had a bug in validating the `redirect_uri` in the `/openid_connect/authorize` endpoint, which allowed specially crafted subdomains to be incorrectly validated when they began with a valid hostname. For example, a `redirect_uri` with a hostname of `agency.gov.example.com` would validate a URL as if it were presented as `agency.gov`.

This enabled an attacker to compromise user sessions on sites that integrated with login.gov. No user interaction was required other than the user being redirected to a URL.

Login.gov immediately patched this bug by making validation of the `redirect_uri` significantly stricter by enforcing an exact match of the hostname. Shortly after, Login.gov worked with agency partners to identify every full URL that agency service providers (SPs) would need to register, and then implemented exact matching for the entire `redirect_uri` (including the URL path).

### SUMMARY BY CABLEJ\_DDS



An error in parsing redirect urls during the authorization flow allowed an attacker to compromise a user's Login.gov token by redirecting users to a malicious site. Props to the TTS team for quickly issuing a patch after the report!

Ineligible for bounty due to government employment.

### TIMELINE · EXPORT



- cablej\_dds submitted a report to TTS Bug Bounty.

Jul 19th (about 1 year ago)
- brodygov posted a comment.

Jul 19th (about 1 year ago)
- brodygov posted a comment.

Jul 20th (about 1 year ago)
- cablej\_dds posted a comment.

Jul 20th (about 1 year ago)
- chessmast3r HackerOne staff changed the status to Triaged.

Jul 23rd (about 1 year ago)
- TTS Bug Bounty has decided that this report is not eligible for a bounty.







Aug 7th (12 months ago)
- cablej\_dds posted a comment.

Aug 15th (12 months ago)
- cablej\_dds posted a comment.

Oct 2nd (10 months ago)
- ericmillgsa posted a comment.

Oct 2nd (10 months ago)
- cablej\_dds posted a comment.

Oct 10th (10 months ago)

 <a href="#">ericmillgsa</a> closed the report and changed the status to  <b>Resolved</b> .	Nov 1st (9 months ago)
 <a href="#">cablej_dds</a> posted a comment.	Nov 5th (9 months ago)
 <a href="#">ericmillgsa</a> requested to disclose this report.	Nov 6th (9 months ago)
 <a href="#">cablej_dds</a> agreed to disclose this report.	Nov 6th (9 months ago)
 This report has been disclosed.	Nov 6th (9 months ago)