

## SUMMARY BY TTS BUG BOUNTY



Login.gov had a bug in validating the redirect\_uri in the <code>/openid\_connect/authorize</code> endpoint, which allowed specially crafted subdomains to be incorrectly validated when they began with a valid hostname. For example, a <code>redirect\_uri</code> with a hostname of <code>agency.gov.example.com</code> would validate a URL as if it were presented as <code>agency.gov</code>.

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 <a href="redirect\_uri">redirect\_uri</a> 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 <a href="redirect\_uri">redirect\_uri</a> (including the URL path).

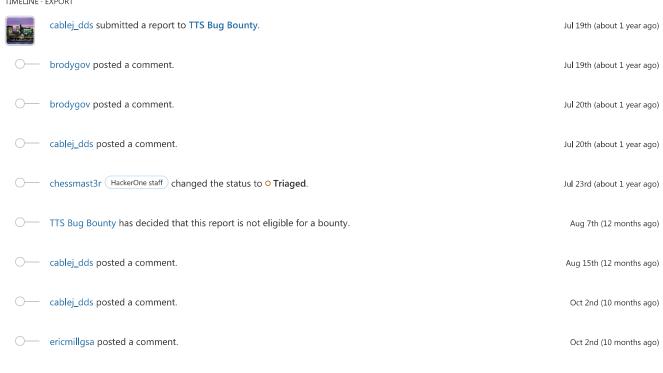
## SUMMARY BY CABLEJ\_DDS



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 posted a comment.

Oct 10th (10 months ago)

ericmillgsa closed the report and changed the status to O Resolved.	Nov 1st (9 months ago)
cablej_dds posted a comment.	Nov 5th (9 months ago)
— ericmillgsa requested to disclose this report.	Nov 6th (9 months ago)
cablej_dds agreed to disclose this report.	Nov 6th (9 months ago)
— This report has been disclosed.	Nov 6th (9 months ago)