

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

07/21/2016

SUBJECT:

A Vulnerability in CGI Based Web Products Could Allow For Unauthorized Redirection of Traffic

OVERVIEW:

A vulnerability has been discovered in a wide variety of Common Gateway Interface (CGI) based web products, which could allow for unauthorized redirection of traffic. This vulnerability exists due to a flaw in the use of the HTTP Proxy environment variable. This vulnerability can be exploited to perform remote man in the middle attacks, cause Denial of Service (DoS) conditions on the affected server, or leverage the affected server to perform Distributed Denial of Service (DDoS) attacks on a third party target.

THREAT INTELLIGENCE:

Due to the open disclosure of this vulnerability, it is likely being exploited in the wild, however the MS-ISAC is not aware of any specific instances.

SYSTEMS AFFECTED:

Many applications and systems with a reliance on CGI or CGI-like environments are affected, as well as those running PHP or third party CGI frameworks. Here are a few that have already released security bulletins regarding this vulnerability:

- Apache
- Drupal
- Go
- IIS
- NGINX
- PHP
- Python

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**

- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability has been discovered in a wide variety of CGI-based web products, which could allow for unauthorized redirection of traffic. This vulnerability exists due to a flaw in the use of the HTTP Proxy environment variable. This vulnerability can be exploited when application code is running on CGI or a CGI-like server. HTTP request headers are merged into a specific variable under keys beginning with HTTP. This information is what getenv reads from. When a user submits a request that contains a Proxy header, the header appears to the application as getenv('HTTP_PROXY'). Some common application libraries are trusting this value, even when run in a CGI/SAPI environment.

This vulnerability can be exploited to perform remote man in the middle attacks, cause Denial of Service (DoS) conditions on the affected server, or leverage the affected server to perform Distributed Denial of Service (DDoS) attacks on a third party target.

RECOMMENDATIONS:

The following actions should be taken:

- Block the Proxy header for applications running PHP or CGI.
- Apply appropriate patches provided by vendors immediately after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying the patch.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the principle of Least Privilege to all systems and services.

REFERENCES:

HTTProxy:

<https://httpoxy.org/>

Drupal:

<https://www.drupal.org/SA-CORE-2016-003>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5385>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5386>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5387>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5388>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1000109>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1000110>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>