

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:

08/26/2016

SUBJECT:

A Vulnerability in FortiGate Firmware Could Allow Security Bypass

OVERVIEW:

FortiGate firmware (FortiOS) released before Aug 2012 has a cookie parser buffer overflow vulnerability. FortiOS is the operating system used by FortiGate network security platforms. This vulnerability, when exploited by a crafted HTTP request, can result in execution control being taken over.

THREAT INTELLIGENCE:

This vulnerability has been publicly disclosed and a tool exists to perform the exploit. There are currently no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

FortiGate (FortiOS):

𔅘.3.8 and below

𔅘.2.12 and below

𔅘.1.10 and below

FortiSwitch:

𔅗.4.2 and below

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: N/A

TECHNICAL SUMMARY:

FortiGate firmware (FortiOS) released before Aug 2012 has a cookie parser buffer overflow vulnerability. This vulnerability, when exploited through a maliciously crafted HTTP request, allows a malicious actor to replace the EGBL.config file with their own allowing execution control being taken over.

Work Arounds/Mitigating Details:

- The following AV and IPS signatures block the potential attacks:
 - ELF/Adows.A!exploit since AV DB 36.803
 - IPS signature: FortiGate.Cookie.Buffer.Overflow since IPS DB 8.935

FortiOS:

- Disable admin access via HTTP and HTTPS on all interfaces, and use SSH instead
- On 4.3, if HTTP or HTTPS access is mandatory, one can restrict access to HTTP and HTTPS to a minimal set of authorized IP addresses, via the Local In policies
- On 4.2 and 4.1, if HTTP or HTTPS access is mandatory, one can restrict access to the administration interfaces (including HTTP and HTTPS access) to a minimal set of authorized IP addresses, via the trusthost commands

FortiSwitch:

- Disable admin access via HTTP and HTTPS on all interfaces, and use the CLI instead. Alternatively, restrict access to the administration interfaces (including HTTP and HTTPS access) to a minimal set of authorized IP addresses, via the 'trusthost' commands

RECOMMENDATIONS:

The following actions should be taken:

- Install appropriate updates or follow mitigation/workaround steps provided by Fortigate after appropriate testing.
 - Upgrade to release 5.x;
 - Upgrade to release 4.3.9 or above for models not compatible with FortiOS 5.x;
 - FortiSwitch: Upgrade to release 3.4.3.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit administrative access to trusted hosts for the affected products.

REFERENCES:

FortiGuard:

<http://fortiguard.com/advisory/cookie-parser-buffer-overflow-vulnerability>

TLP: WHITE

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

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