

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.

DATE(S) ISSUED:

09/26/2013

SUBJECT:

Denial Of Service Vulnerability in Blue Coat Proxy SG and Security Gateway OS

OVERVIEW:

A Denial of Service (DoS) vulnerability has been reported in Blue Coat Proxy SG and Security Gateway OS. Blue Coat Proxy allows for policy control over web-based traffic based on content, users, applications and protocols. Blue Coat Security Gateway OS is the operating system that runs on Blue Coat appliances to allow for security services to run. Successful exploitation of this vulnerability could result in denial of service conditions.

SYSTEMS AFFECTED:

- SGOS versions prior to 6.5.2 except version 6.2.14.1

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

DESCRIPTION:

Bluecoat has reported that there is a vulnerability in Blue Coat Proxy SG and Security Gateway OS that could allow Denial of Service (DoS) conditions. This vulnerability is due to a memory leak that could be used to force a Proxy SG appliance to drop or bypass traffic. This can be triggered remotely by distributing spam email or similar mechanisms where the target user clicks through to a site that can trigger the memory regulation issue. When Proxy SG forward or reverse proxy of HTTP traffic is enabled, the system may experience memory regulation and require a reboot when running a proxy on a high number of HTTP RW pipeline pre-fetch

requests. The system will either drop or block all subsequent proxy connections until a reboot is performed.

All SGOS versions prior to 6.5.2 except version 6.2.14.1 are vulnerable in both forward and reverse proxy modes. This has no impact on Management Console, command line interface, or administrative functions.

Successful exploitation of this vulnerability could result in Denial of Service conditions requiring a reboot of the affected system.

Proxy SG Patch Information:

- SGOS 6.5 – A fix is available in 6.5.2, which sets a maximum prefetching memory allocation size. This forces a timeout and retry when there are too many requests for HTTP proxy services. The fix is available to customers with a valid Blue Touch Online login.
- SGOS 6.4 – A fix is not yet available as of 6.4.4.1.
- SGOS 6.3 – A fix is not yet available as of 6.3.6.1.
- SGOS 6.2 – A fix is available in 6.2.14.1, which sets a maximum prefetching memory allocation size. This forces a timeout and retry when there are too many requests for HTTP proxy services. The fix is available to customers with a valid BlueTouch Online login from <https://bto.bluecoat.com/download/product/7375>.
- SGOS 6.1 – A fix is not yet available as of 6.1.6.3.
- SGOS 5.5 – A fix is not yet available as of 5.5.11.3.
- SGOS 5.4 – A fix is not yet available as of 5.4.12.6.
- Proxy SG 5.3 and earlier – please upgrade to a later version.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade vulnerable Blue Coat products immediately after appropriate testing

REFERENCES:

Bluecoat:

<https://kb.bluecoat.com/index?page=content&id=SA75>

SecurityFocus:

<http://www.securityfocus.com/bid/62647>