



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

January 14, 2009

The following cyber advisory was issued by the State of Alaska and was 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.

STATE OF ALASKA ADVISORY NUMBER:

2009-002

DATE(S) ISSUED:

01/14/09

SUBJECT:

Cisco IOS Cross-Site Scripting Vulnerabilities

OVERVIEW:

This response covers two separate cross-site scripting vulnerabilities within the Cisco IOS Hypertext Transfer Protocol (HTTP) server (including HTTP secure server - here after referred to as purely HTTP Server) and applies to all Cisco products that run Cisco IOS Software versions 11.0 through 12.4 with the HTTP server enabled. A system that contains the IOS HTTP server or HTTP secure server, but does not have it enabled, is not affected.

RISK: Moderate

DESCRIPTION:

This response covers two separate cross-site scripting vulnerabilities within the Cisco IOS Hypertext Transfer Protocol (HTTP) server (including HTTP secure server - here after referred to as purely HTTP Server) and applies to all Cisco products that run Cisco IOS Software versions 11.0 through 12.4 with the HTTP server enabled. A system that contains the IOS HTTP server or HTTP secure server, but does not have it enabled, is not affected.

To determine if the HTTP server is running on your device, issue the `show ip http server status | include status` and the `show ip http server secure status | include status` commands at the prompt and look for output similar to:

```
Router#show ip http server status | include status
```

```
HTTP server status: Enabled  
HTTP secure server status: Enabled
```

If the device is not running the HTTP server, you should see output similar to:

```
Router#show ip http server status | include status
```

```
HTTP server status: Disabled  
HTTP secure server status: Disabled
```

These vulnerabilities are documented in the following Cisco bug IDs:

- Cisco bug ID CSCsi13344 - XSS in IOS HTTP Server
Special Characters are not escaped in URL strings sent to the HTTP server.

- Cisco bug ID CSCsr72301 - XSS in IOS HTTP Server (ping parameter)
Special Characters are not escaped in URL strings sent to the HTTP server, via the ping parameter. The ping parameter is used both by external applications such as Router and Security Device Manager (SDM) as well as a direct HTTP session to Cisco IOS http server. This vulnerability affects 12.1E based trains and all Cisco IOS releases after 12.2(13)T.

These vulnerabilities are independent of each other. For a full solution, download a Cisco IOS version that contains the fixes for both Cisco bug IDs. These vulnerabilities have been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-3821.

Workaround:

If the HTTP server is not used for any legitimate purposes on the device, it is a best practice to disable it by issuing the following commands in configure mode:

```
no ip http server
no ip http secure-server
```

If the HTTP server is required, it is a recommended best practice to control which hosts may access the HTTP server to only trusted sources. To control which hosts can access the HTTP server, you can apply an access list to the HTTP server. To apply an access list to the HTTP server, use the following command in global configuration mode:

```
ip http access-class {access-list-number | access-list-name}
```

The following example shows an access list that allows only trusted hosts to access the Cisco IOS HTTP server:

```
ip access-list standard 20
permit 192.168.1.0 0.0.0.255
remark "Above is a trusted subnet"
remark "Add further trusted subnets or hosts below"
```

```
! (Note: all other access implicitly denied)
! (Apply the access-list to the http server)
```

```
ip http access-class 20
```

REFERENCES:

Cisco:

http://www.cisco.com/en/US/products/products_security_response09186a0080a5c501.html