Cisco IOS AAA WEB_EXEC Command Authorization Security Bypass

Ref ID	NCIT-SB-2012-06	**Vulnerability Identifier**	CISCO Customers
Description	Vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.		
Impact	Confidentiality **(High)**	Integrity **(High)**	Availability **(High)**
Vulnerability Type	Execute Code, Bypass a restriction or similar		
Release Date	March 29, 2012	**Last Update Date**	April 03, 2012

Affected Vendors

The HTTP server is enabled by default for cluster configurations and on the following Cisco switches: Catalyst 3700 series, Catalyst 3750 series, Catalyst 3550 series, Catalyst 3560 series, and Catalyst 2950 series.

Solution:

Cisco has released free software updates that addresses the vulnerability described in this advisory. Prior to deploying software, customers are advised to consult their maintenance providers or check the software for feature set compatibility and known issues that are specific to their environments.

Customers may only install and expect support for feature sets they have purchased. By installing, downloading, accessing, or otherwise using such software upgrades, customers agree to follow the terms of the Cisco software license at http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html, or as set forth at http://www.cisco.com/public/sw-center/sw-usingswc.shtml.

References

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai