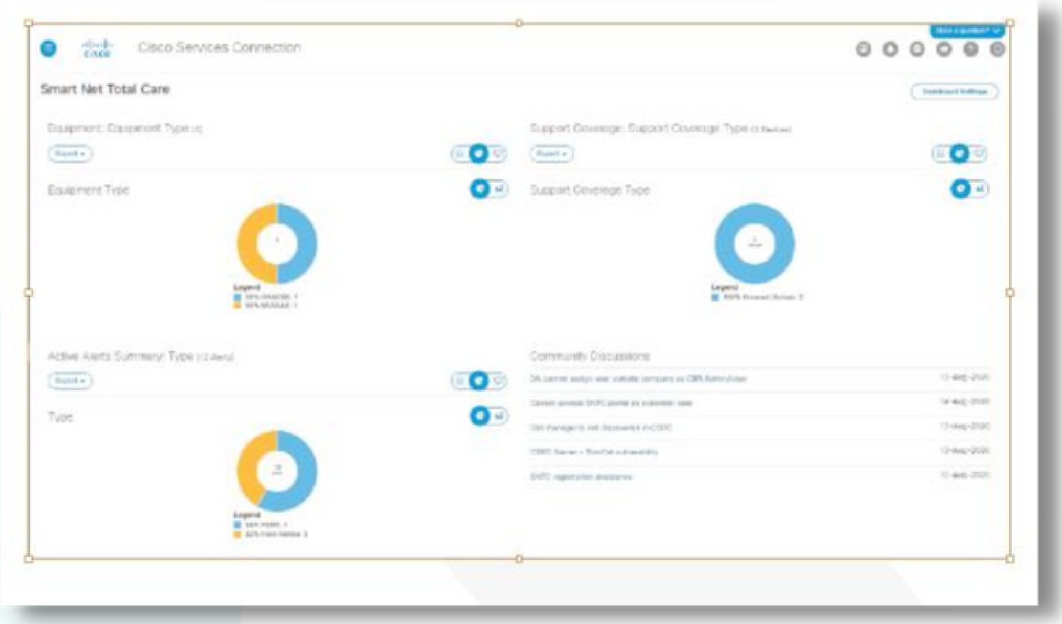
aap3 /// 2023

CISCO NETWORK AUDIT SERVICE

info@aap3.com
uk.aap3.com/
aap3
02380 762 800

With so much depending on your network, a security breach or routine maintenance issue can have a major effect on your customers, your employees and your business. Your IT infrastructure is the link that connects your business to customers and suppliers. Business success requires optimal service levels on your network whilst reducing costs and expanding your network as your business grows. aap3 Cisco Network Audit Service and our other foundational services help you meet these objectives.

aap3 Cisco Network Audit Service is delivered through the Cisco Services Connection portal providing actionable information and automation to support your Cisco products. Customizable screens show you current status about security and product alerts, service coverage, product lifecycles and historical TAC support information.


Cisco Services Connection
Smart Net Total Care
Equipment: Equipment Type
Support Coverage: Support Coverage Type
Equipment Type
Support Coverage Type
Legend
Active Alerts Summary: Type
Type
Community Discussions

aap3 will install a Cisco Smart collector (CSPC) onto your network estate which automatically gathers device support information for Cisco products including serial numbers, installed cards, modules and product IDs. This saves significant amounts of time and provides a live current view compared with manual efforts. The collector also identifies hardware and software versions for your Cisco network devices.

Once this is captured and uploaded to the portal, you will be provided with interactive workflows that simplify support management processes. Altogether, the foundational technical services and smart capabilities work to provide the visibility and insight you need to improve the efficiency of your support operations, resolve problems immediately and mitigate security risk.

ASSET LIST

Networks are continuously expanding and for all businesses knowing what devices you have on your network can be complex. The collector solves this challenge by providing you with a live inventory of all Cisco assets.

SECURITY ADVISORY

Threats increase every day, but how do you know what devices are vulnerable? A Cisco Smart Collector provides you with a list of each device and what security notices are applicable.

END OF SUPPORT NOTIFICATIONS

As Cisco's product portfolio grows, devices become End of Support and planning for this can be difficult. The Cisco Smart Collector provides you with this insight so that you can start to plan your refresh cycles.

COVERAGE

How do I know if my device is covered by a support contract? A Smart Collector shows you.

CONTRACT INFORMATION

- Start date
- End date
- Active, overdue or expired
- Contract number

SOFTWARE VERSIONS

The smart collector will provide you with the software version that is running on which devices ensuring software version consistency across your Cisco estate.

TAC CASE SUPPORT

The Smart Collector portal is one of four ways you can create a TAC case accelerating your TAC case creation.

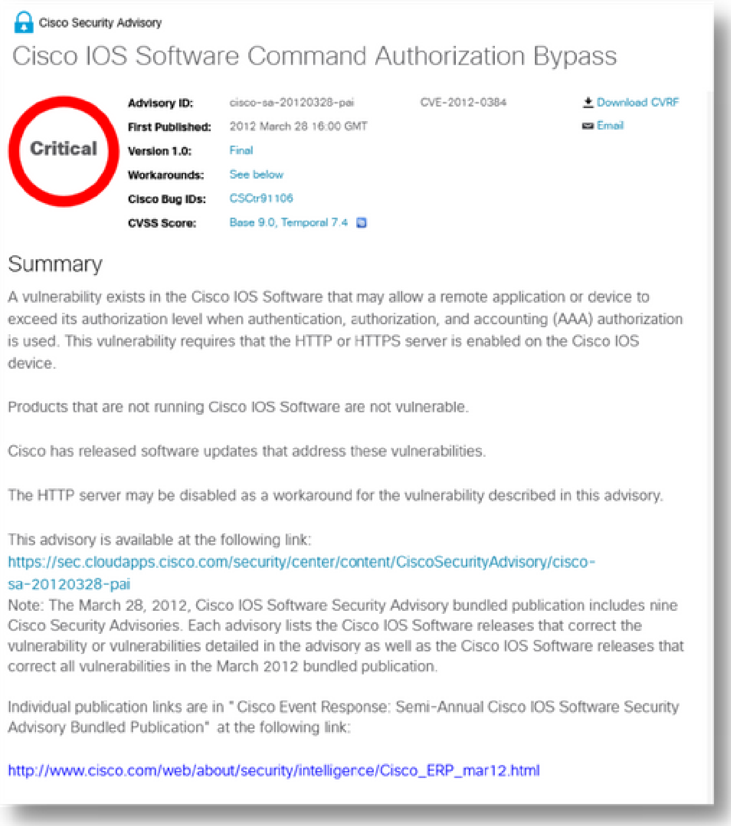
ACCESS MANAGEMENT

The Smart Collector can have access levels applied to users that require different levels of access such as partners, administrators and users.

Security and product alerts –
Know the security and product alerts that affect your network

Staying current with Cisco alerts regarding security recommendations, hardware updates and software releases can be challenging. Smart capabilities help pre-empt network disruption by allowing you to identify and manage relevant alerts for your devices. They proactively identify which devices are affected by Cisco published product alerts and security advisories and enable you to report alert related activity.

Alert information is available for hardware, software and security alert and field notices. An alert management workflow allows you to assign status information to alerts. It then filters future alerts so that you only receive those that still require your attention. If you close an alert, or change its status to 'action taken', you will not be distracted by that alert in the future. Alert status information also makes it easy for supervisors to monitor your team's progress toward desired goals as they work on reviewing alerts and performing the required actions.



Cisco Security Advisory

Cisco IOS Software Command Authorization Bypass

Advisory ID:	cisco-sa-20120328-pai	CVE-2012-0384	Download CVRF
First Published:	2012 March 28 16:00 GMT		Email
Version 1.0:	Final		
Workarounds:	See below		
Cisco Bug IDs:	CSCtr91106		
CVSS Score:	Base 9.0, Temporal 7.4		

Summary

A 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.

Products that are not running Cisco IOS Software are not vulnerable.

Cisco has released software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai
Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in " Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

Service coverage management –
Identify what is and what is not covered

Without visibility of your installed base and service contract status there is a risk that an uncovered device will have an outage leaving you scrambling to find a solution while your network is compromised. The portal reports help ensure that your business critical assets have the necessary service coverage to meet business needs and comply with corporate policies.

The portal provides automated installed base and contract management functionality to assist you in determining the correct coverage for your Cisco devices. Whereas manual methods of tracking service coverage for large or complex networks can be time consuming and prone to error, SmartNet uses automation to save time and reduce risk. Regular data collection and flexible reporting capabilities help you manage your Cisco installed base and service contracts, identifying and tracking what is new, what's changed and what's covered.

Product lifecycle management –
Obtain the information to plan for product replacements and upgrades

Using up-to-date data from the portal provides dramatic efficiencies over maintaining spreadsheets whilst also reducing errors. The portal reports help you maintain a current view of your Cisco installed base, including device configuration details such as serial number, product ID, Cisco IOS® software version, installed memory and firmware, IP address and hostname. Up-to-date records on coverage also helps simplify your renewal and budget planning processes. SmartNet allows you to quickly identify service contracts that will expire at various intervals so that you can plan for renewals and identify budget requirements.

By providing enhanced visibility into your installed base you can:

- Quickly identify Cisco products that are reaching end of life, end of sale, or end of support
- Easily see what has been moved, added, or changed in your network
- Verify that your Cisco hardware is running current, consistent and supported software versions
- Mitigate risk and plan for upgrades for equipment that are no longer supported