GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

14 July 2026

Advisory 165: CVE-2008-4128 — Cisco IOS Cross-Site Request Forgery Vulnerability

Release Date: 13th July 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2008-4128 describes multiple cross-site request forgery (CSRF) vulnerabilities in the HTTP Administration component in Cisco IOS 12.4 on the 871 Integrated Services Router, allowing remote attackers to execute arbitrary commands via a certain "show privilege" command to the `/level/15/exec/-` URI, and a certain "alias exec" command to the `/level/15/exec/-/configure/http` URI.

What are the systems affected?

The known affected software configuration is Cisco IOS version 12.4 running on the Cisco 871 Integrated Services Router.

What does this mean?

How it's exploited:

The attack requires the following conditions to be met simultaneously:

- The Cisco 871 router has its HTTP Administration interface enabled and reachable
- An administrator is actively authenticated to the router's web interface in an open browser session
- The administrator can be induced into visiting a malicious page or following a crafted link

Step 1 — Reconnaissance
The attacker identifies a Cisco 871 router running IOS 12.4 with the HTTP administration interface accessible on the network.

Step 2 — Crafting the Forged Request
The attacker crafts malicious HTTP requests targeting the privileged level 15 URI paths. The two specific attack vectors confirmed by NVD are:

Vector 1: GET /level/15/exec/-
→ Executes "show privilege" — reveals admin privilege level

Vector 2: GET /level/15/exec/-/configure/http
→ Executes "alias exec" command — can create persistent command aliases for backdoor access

Step 3 — Delivery to the Authenticated Administrator
The attacker delivers the forged request by embedding it in a malicious web page, phishing email, or hidden image tag that the authenticated admin loads while their router session is active. The browser automatically sends the request — including the admin's active session cookie — to the router.

Step 4 — Execution
The router, receiving what appears to be a legitimate authenticated request, executes the embedded IOS command at privilege level 15 — full administrative authority. The administrator has no visibility that the command was executed.

Mitigation process

CERTVU recommends the following:

Primary — Replace End-of-Life Hardware
Since the Cisco 871 ISR and Cisco IOS 12.4 are both end-of-life, no vendor patch will be issued. Cisco IOS Software releases 12.4 mainline are now classified as obsolete. The definitive remediation is to replace the device with a currently supported Cisco platform running a maintained IOS XE release.

Secondary — Disable the HTTP Administration Interface
Remove the attack vector entirely by disabling the HTTP server:

```
Router(config)# no ip http server
Router(config)# no ip http secure-server
```

Disabling the HTTP Server feature eliminates the attack vector for this vulnerability and may be a suitable mitigation until affected devices can be upgraded. Administrators can disable the HTTP Server feature by using the `no ip http server` or `no ip http secure-server` command in global configuration mode.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2008-4128

.