DRONA
CYBER SOLUTIONS

DRONA CYBER SOLUTIONS PVT LTD

CISCO IOS CROSS SITE REQUEST FORGERY (CSRF)

An advanced threat advisory detailing CVE-2008-4128, a high-impact configuration hijacking vulnerability currently listed in the Known Exploited Vulnerability (KEV) Catalog and aggressively exploited globally by state-sponsored threat groups.

Drona Cyber Solutions Pvt Ltd	July 17, 2026	HIGH: RED
PREPARED BY	*DATE OF ISSUE*	*CLASSIFICATION MATRIX*

www.dronacybersolutions.com

Security Vulnerability Advisory (CVE-2008-4128)

SEVERITY: MEDIUM

Issued By: **Drona Cyber Solutions Pvt Ltd** | Source: **Drona Threat Intel**

EXECUTIVE SUMMARY

Drona Threat Intel has released this specialized Security Update Advisory to highlight ongoing state-sponsored activities targeting legacy networks. Specifically, this advisory focuses on a critical vulnerability within Cisco Internetwork Operating System (IOS) that continues to serve as an entry point for advanced persistent threats (APTs). The Common Vulnerabilities and Exposures (CVE) database and the Common Vulnerability Scoring System (CVSS) characterize this issue as a medium-severity risk, yet its real-world exploitation profile makes its mitigation critical.

> **[CRITICAL WARNING: CONSOLE SECURITY ALERT]**
>
> **Active exploitation vector:** Russian FSB Center 16 threat actors are utilizing Cross-Site Request Forgery (CSRF) via CVE-2008-4128 alongside weak SNMP credentials to copy running configurations and establish deep, persistent command execution boundaries inside critical enterprise infrastructure.

ATTACK CHAIN & DISTRIBUTION METHOD

Analysis from Drona Threat Intel indicates that Russian Federal Security Service Center 16 cyber actors (operating under aliases such as Berserk Bear, Energetic Bear, Ghost Blizzard, and Static Tundra) utilize a highly targeted exploit chain:

- **Target Identification & Scanning:** Attackers scan internet-facing Cisco routing hardware to find systems with poorly secured HTTP administration portals or default SNMP community strings.
- **Malicious Page Hosting:** Threat actors construct custom, malicious web portals designed to trigger hidden, authenticated configuration requests on the router.
- **User Trickery & Exploitation:** An authenticated network administrator is lured into visiting the malicious page, causing the browser to send unauthorized command requests directly to the Cisco HTTP Administration service.
- **Unauthorized Privilege Escalation:** The request executes administrative commands, enabling privilege escalation to level 15 or establishing system configuration command aliases.

Technical Deep Dive & Core Analysis

Intelligence Profile: **FSB Center 16 Operational Blueprint**

TECHNICAL ANALYSIS OF CORE CAPABILITIES

The underlying vulnerability, CVE-2008-4128, affects the HTTP Administration component of **Cisco IOS 12.4 on the 871 Integrated Services Router**. If web administration is enabled without sufficient cross-site request validation controls, a crafted HTTP request can execute configuration actions with the privileges of the active session.

Drona Threat Intel has validated two high-impact attack paths that do not require credentials:

- **Privilege Escalation Commands:** Triggering a "show privilege" query through level 15 permissions, exposing administrative paths.
- **Alias Execution Injection:** Injecting custom system alias exec commands to control routing paths and configurations via simple, unauthenticated background web traffic.

STRATEGIC RECOMMENDATIONS & MITIGATIONS

Drona Threat Intel recommends that all network administrators immediately apply the following mitigations to disrupt Center 16 capabilities:

Mitigation Requirement	Implementation Details
DECOMMISSION AND REPLACE	**Retire end-of-life Cisco 871** routers immediately. These devices have reached official End-of-Support and cannot receive security updates.
DISABLE HTTP INTERFACE	**Disable Cisco HTTP administration** where web management is unnecessary. Restrict authorized management via strict Access Control Lists.
ENFORCE SNMPv3 ONLY	**Decommission legacy SNMPv1/v2c** immediately. Implement SNMPv3 with authPriv mode and strong, distinct passphrases.
DISABLE CISCO SMART INSTALL	**Execute the global "no vstack"** configuration command to disable the Smart Install feature and remove its exposed TCP 4786 listening port.

INDICATORS OF COMPROMISE (IOCS)

Target System / Vector	Type	Operational Context
`Cisco IOS 12.4 (871 ISR)`	Vulnerable OS	Affected firmware version harboring HTTP administration flaws.
`OID 1.3.6.1.4.1.9.9.96.1.1`	SNMP Object ID	Monitored for unauthorized configuration copy actions to TFTP hosts.
`UDP Port 69 / TCP Port 4786`	Network Ports	Inbound/Outbound vectors used for configuration exfiltration & Smart Install.