Cynamics

Protect From Cisco IOS XE Hack In 5 Minutes Using Cynamics AI

cynamics.ai

A few days ago, Cisco revealed a significant hack in their IOS software.[1] You can follow these steps to determine if this exploitation has infected your device.[2] Our immediate recommendation and best practice is disabling the feature (see commands for disabling in the link).

The vulnerability is affecting Cisco routers and switches running IOS XE:

Controllers	Cisco Catalyst 9800 Series Wireless Controllers
Switches	Cisco Catalyst® 9500, 9400, 9300, 3850, and 3650
Aggregation/edge routers	ASR1013, ASR1009-X, ASR1006-X, ASR1006, ASR1004-X, ASR1002-HX, ASR1001-HX, ASR1002-X, and ASR1001-X
Branch routers	4451 ISR, 4431 ISR, 4351 ISR, 4331 ISR, 4321 ISR, 4221 ISR, and 1000 ISR
Virtual routers	CRS 1000v, ISRv

Immediate Mitigation Action-items

Now, and more than usual, network segregation is critical and can be the key to effectively containing the potential attacker. We'd recommend the following:

- Ensure a solid air gap between WiFi subnets and core subnets.
- Allow only the network admin IP/s or subnets and only them to connect to the Cisco devices.

Moreover, in many cases, we saw how 3rd party IT shops have wrongly allowed a public interface connection to the Cisco devices, for example, to accept a remote web login. While it has always been a bad security practice, this hack is even more critical and might allow the bad actor to access your network's core.

[1] https://www.crn.com/news/security/cisco-ios-xe-hack-researchers-find-another-sharp-increase-in-affected-devices

[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z#vp

Thus, we'd recommend the following:

- First, if you have a device listed above directly connected to the public internet, it is already at high risk from an internal access breach. Make sure to close the HTTP/s connection on the device.
- Specifically, ensure all switches are internal, do not have a public IP, and use a private IP management interface.

Cynamics to the Rescue

Cynamics is the only network detection and response (NDR) solution that can cover the entire network, no matter how big or complex. Its unique sample-based approach, collecting much less than 1% of the network traffic from main gateways and learning from them about the entire 100% network, enables organizations of all sizes and architectures to have complete network coverage, visibility, and threat prediction in just a few minutes, without installing even one appliance or agent.

Cynamics proprietary AI technology analyzes network patterns in different layers - from the gateways through significant assets down to the endpoints and predicts attacks, threats, and anomalies long before they hit. This is the answer to the new hack.

You can now create your Cynamics account free of charge and connect your Cisco device to Cynamics in a few minutes. Immediately after, Cynamics AI will analyze your network and detect any attack or threat due to the IOS XE hack. With Cynamics you will get a complete and immediate network coverage and protection from this hack, among other threats, malicious campaigns, and full network coverage.