Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security
Centre

Routers targeted: Cisco Smart Install feature continues to be targeted by Russian state-sponsored actors

State sponsored actors

iOS

Russian state-sponsored actors are responsible for activity targeting Cisco devices using the Smart Install feature worldwide, including Australia.

Cisco has published the actions needed to secure the Smart Install feature in, Action Required to Secure the Cisco IOS and IOS XE Smart Install Feature.

The ACSC has previously released guidance on cyber adversaries targeting this feature to extract configuration files from routers and switches of a number of Australian organisations.

Preventing malicious activity

Organisations are advised to identify Cisco devices running Smart Install within their networks, evaluate the need of running this feature, and remove or secure the feature as required. Both the ACSC and Cisco documentation contain details on how to accomplish this.

Related information

- Australian Government Minister for Law Enforcement and Cyber Security media release: Australian Government attribution of cyber incident to Russia
- UK NCSC Advisory: Russian state-sponsored cyber actors targeting network infrastructure devices

- UK NCSC: Joint US-UK statement on malicious cyber activity carried out by Russian government
- US CERT: Joint US-UK Technical Alert TA18-106A

Contact

If you find any evidence of this activity, report the incident to the ACSC via email or call the 24/7 Hotline for urgent assistance on 1300 CYBER1 (1300 292 371)