Don’t take BADCANDY from strangers – How your devices could be implanted and what to do about it

First published: 31 October 2025

Last updated: 31 October 2025

Overview

BADCANDY

Cyber actors are installing an implant dubbed ‘BADCANDY’ on Cisco IOS XE devices that are vulnerable to CVE-2023-20198. Variations of the BADCANDY implant have been observed since October 2023, with renewed activity notable throughout 2024 and 2025.

BADCANDY is a low equity Lua-based web shell, and cyber actors have typically applied a non-persistent patch post-compromise to mask the device’s vulnerability status in relation to CVE-2023-20198. In these instances, the presence of the BADCANDY implant indicates compromise of the Cisco IOS XE device, via CVE-2023-20198.

The BADCANDY implant does not persist following a device reboot however, where an actor has accessed account credentials or other forms of persistence, the actor may retain access to the device or network. The patch for CVE-2023-20198 must be applied to prevent re-exploitation. Access to the web user interface should also be restricted if enabled (see the *General Hardening* section below).

Since July 2025, ASD assesses over 400 devices were potentially compromised with BADCANDY in Australia. As at late October 2025, there are still over 150 devices compromised with BADCANDY in Australia.

CVE-2023-20198

This critical vulnerability affects the web user interface (UI) feature of Cisco IOS XE Software. Exploitation of this vulnerability could allow a remote, unauthenticated user to create a highly privileged account on the vulnerable system, allowing them to take control of the system.

This vulnerability has been leveraged by actors such as SALT TYPHOON and was one of the top routinely exploited vulnerabilities in 2023.

ASD is aware of ongoing exploitation.

Actor Attribution

While any actor can use this implant, ASD believes that criminal and state sponsored cyber actors may leverage the BADCANDY implant. Cyber actors are known to re-exploit previously compromised devices where the device has not been patched and the interface has been left exposed to the internet. This presents an ongoing risk to Australian networks.

ASD's Response

ASD has sent victim notifications to entities via their service provider if ASD cannot determine the system operator. These notifications contain instructions to patch and reboot the device, perform hardening and, conduct incident response on any impacted devices.

ASD will continue to conduct victim notifications to ensure system operators are aware that their device has been compromised.

What You and Your Organisation Can Do

ASD recommends that system operators take the following actions to remove the BADCANDY implant if compromised and to mitigate the risk of re-exploitation. These actions will not only assist organisations, but will help reduce the number of devices compromised with the BADCANDY implant in Australia.

- Review the running configuration for accounts with privilege 15 and remove unexpected or unapproved accounts.
- Accounts with random strings or "cisco_tac_admin", "cisco_support", "cisco_sys_manager", or "cisco" should also be reviewed and removed if not legitimate.

- Review the running configuration for unknown tunnel interfaces. Tunnels appear in the running configuration as “interface tunnel[number]” followed by the IP address, tunnel source, and tunnel destination.
- If enabled, review TACACS+ AAA command accounting logging for configuration changes for these compromised devices.

Patch against CVE-2023-20198

All Australian organisations using the web UI feature of Cisco IOS XE Software are strongly encouraged to apply the patch and follow the recommendations detailed in Cisco’s security advisory:

- Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature

Cisco reports active exploitation of this vulnerability and has published indicators of compromise to assist system owners in investigating for signs of malicious activity.

Reboot your device

As the BADCANDY implant is not persistent, rebooting will remove the implant. However, rebooting will not reverse additional actions taken by the threat actor and will not remedy the initial vulnerability exploited to gain access. The running configuration must be examined for unexpected changes as above.

General hardening

Follow the Cisco advice linked below, particularly in relation to ensuring that the HTTP server feature is disabled. Further, the Cisco IOS XE hardening guide should be followed to mitigate future compromise:

- Cisco IOS XE Software Hardening Guide

Edge devices are critical network components. ASD recommends implementing key strategies for securing edge devices aimed at enhancing network security and reducing vulnerabilities. See the following publication for more:

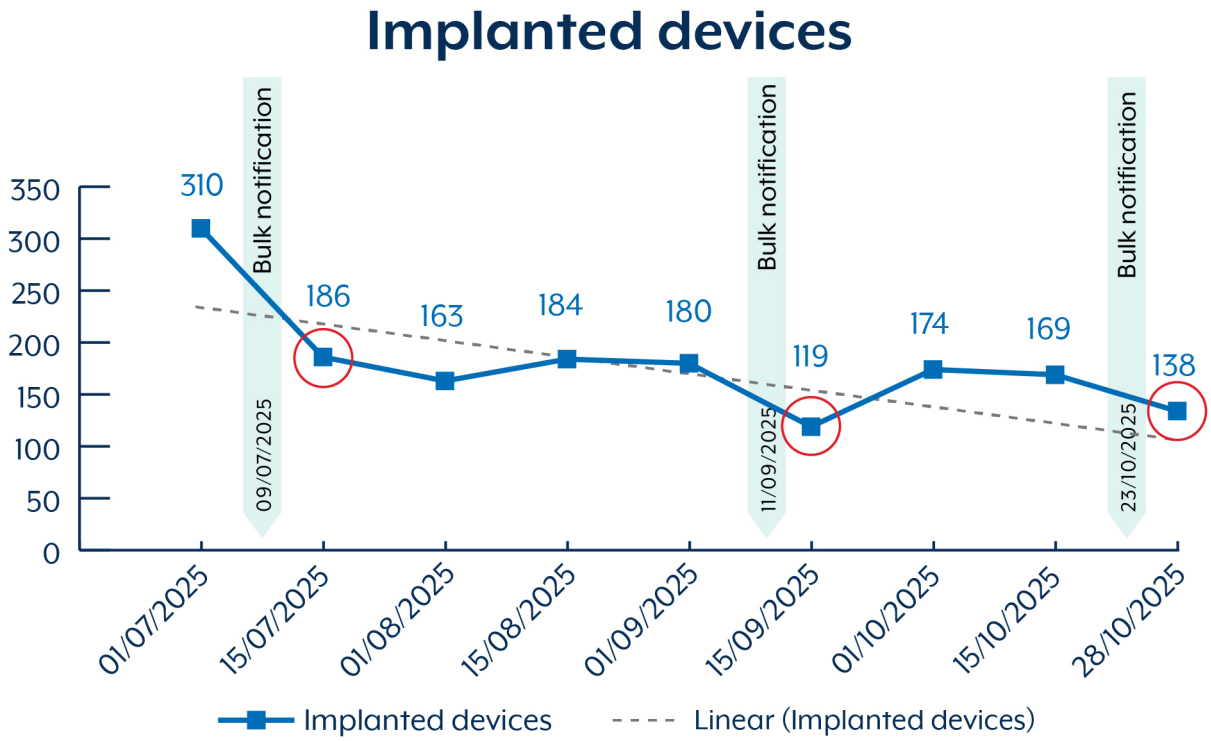
- Securing edge devices | Cyber.gov.au

The Stats

Below is a graph that shows the number of BADCANDY implanted devices from July 2025 to October 2025. ASD has marked when bulk victim notifications took place (labelled as *Bulk Notification)*.

Whilst there has been a steady decline from late October/November 2023 of over 400 compromised devices to under 200 in 2025, we continue to see fluctuations in this data as re-exploitation is likely occurring, including on devices for which ASD has previously issued notifications.

ASD believes actors are able to detect when the BADCANDY implant is removed and are re-exploiting the devices. This further highlights the need to patch against CVE-2023-20198 to avoid re-exploitation.



Resources

- Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerabilities
- Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature
- Cisco IOS XE Software Hardening Guide
- Securing edge devices | Cyber.gov.au
- Mitigations for network defence | Cyber.gov.au.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre