NCSC

National Cyber Security Centre

2310170118-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical severity Cisco IOS vulnerability under active exploitation

Tuesday 17th October, 2023

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP:CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Cisco has released an advisory stating that a previously unknown vulnerability in the web UI of Cisco IOS XE software is under active exploitation. The vulnerability, CVE-2023-20198, has a CVSS severity of 10. This allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access.

No patch or workarounds are available at the time of writing.

Products Affected

This vulnerability affects devices running Cisco IOS XE software with the web UI feature enabled.

Impact

Exploitation of CVE-2023-20198 could allow an attacker to create an account on the device with a privilege level of 15. This can provide the attacker with complete control over the device. Once the account is made, the attacker may drop an implant onto the system resulting in persistent access.

Cisco has reported that this vulnerability is under active exploitation.

Recommendations

The NCSC strongly advises affected organisations to follow Cisco's advice and disable the HTTP server feature on all systems with Internet access. If both the HTTP server and HTTPS server are in use, both commands to disable the HTTP Server feature are required.

Organisations should follow the checks contained within the Indicators of Compromise section of the Cisco advisory in order to determine if their system has been compromised.

Further information and a recommendations guide can be found here:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie