An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2411110189

# NCSC Advisory

## Critical vulnerability exists in Cisco Firepower Threat Defense (FTD) Software: CVE-2024-20412 (CVSSv3: 9.3)

**11th, November 2024**

**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.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

# Description

**CVE ID:** 2024-20412

**Published:** 2024-10-23 16:00 GMT

**Vendor:** Cisco

**Product:** Cisco Firepower Threat Defense

**CVSS3.0[1] Score:** 9.3

**Summary:**

This vulnerability is due to the presence of static accounts with hard-coded passwords on an affected system. An attacker could exploit this vulnerability by logging in to the CLI of an affected device with these credentials. Successful exploitation could allow an unauthenticated, local attacker to access an affected system using static credentials.

# Products affected

This vulnerability may affect the following Cisco products if they are running Cisco FTD Software Release 7.1 through 7.4 with a vulnerability database (VDB) release of 387 or earlier:

- Firepower 1000 Series
- Firepower 2100 Series
- Firepower 3100 Series
- Firepower 4200 Series

# Impact

A successful exploit could allow the attacker to access the affected system and retrieve sensitive information, perform limited troubleshooting actions, modify some configuration options, or render the device unable to boot to the operating system, requiring a reimage of the device.

**Common Weakness Enumeration (CWE)[2]:** CWE-259: Use of Hard-coded Password

**Known Exploited Vulnerability (KEV) catalog[3]**: Not Known

**Used by Ransomware Operators**: Not Known

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://cwe.mitre.org/
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

# Recommedations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Cisco.

Additional recommendations, mitigations, indicators of compromise and workarounds for CVE 2024-20412 can be found in the respective link(s) below:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-statcred-dFC8tXT5