National Cyber Security Centre

2401260171-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Cisco Unified Communications Products Remote Code Execution Vulnerability (CVE-2024-20253)

Friday 26th January, 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.

Description

CVE-2024-20253 is a vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products that could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device.

At the time of writing, Cisco has reported that there is no evidence that CVE-2024-20253 has been exploited in the wild.

Products Affected

- Unified Communications Manager (Unified CM)
- Unified Communications Manager IM & Presence Service (Unified CM IM&P)
- Unified Communications Manager Session Management Edition (Unified CM SME)
- Unified Contact Center Express (UCCX)
- Unity Connection (UC)
- Virtualized Voice Browser (VVB)

Impact

An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device.

Recommendations

The NCSC strongly advises affected organisations to install updates for vulnerable devices with the highest priority, after thorough testing.

Cisco has released free software updates that address the vulnerability. Please see the Cisco advisory for more information.

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm

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