National Cyber Security Centre

2407180181-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in Cisco Secure Email (CVE-2024-20401, CVSSv3: 9.8)

Thursday 18th July, 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

Published: 2024-07-17T17:15:00
Vendor: Cisco
Product: Cisco Secure Email
CVE ID: CVE-2024-20401
CVSS3.0 Score[1]**:** 9.8
EPSS[2]**:** 0.093060000
Summary: A vulnerability in the content scanning and message filtering features of Cisco Secure Email Gateway could allow an unauthenticated, remote attacker to overwrite arbitrary files on the underlying operating system. This vulnerability is due to improper handling of email attachments when file analysis and content filters are enabled. An attacker could exploit this vulnerability by sending an email that contains a crafted attachment through an affected device. A successful exploit could allow the attacker to replace any file on the underlying file system. The attacker could then perform any of the following actions: add users with root privileges, modify the device configuration, execute arbitrary code, or cause a permanent denial of service (DoS) condition on the affected device. **Note:** Manual intervention is required to recover from the DoS condition. Customers are advised to contact the Cisco Technical Assistance Center (TAC) to help recover a device in this condition.

More information related to this issue can be found at the following link:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-bGG2UsjH

Products Affected

- Cisco Cisco Secure Email

Impact

Common Weakness Enumeration (CWE)[3]**:** Absolute Path Traversal

Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** NO

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Cisco. Additional recommendations and mitigations for CVE-2024-20401 can be found in the respective link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-bGG2UsjH

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

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
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre