CERT-EU

Security Advisory 2023-098

SMTP Smuggling Vulnerability in CISCO Secure Email Gateway

December 19, 2023 — v1.0

TLP:CLEAR

History:

- *19/12/2023 — v1.0 – Initial publication*

Summary

On December 18, 2023, researchers from SEC Consult released an article about an SMTP Smuggling vulnerability affecting products from several vendors such as Microsoft, GMX or Cisco [1]. While the vulnerability was fixed in GMX and Microsoft products, it is considered as a feature in Cisco Secure Email Gateway and Cisco Secure Email Cloud Gateway, and thus, it was not fixed.

It is recommended to change the default configurations of the Cisco Secure Email Cloud Gateway and Cisco Secure Email Gateway.

Technical Details

The vulnerability comes from the various interpretations of the end-of-data sequence (`<CR><LF>.<CR><LF>`) in emails. By exploiting this interpretation differences of the SMTP protocol, it is possible to smuggle/send spoofed emails - hence SMTP smuggling - while still passing SPF alignment checks. Two types of SMTP smuggling are possible, outbound and inbound.

Affected Products

Cisco Secure Email Gateway and Cisco Secure Email Cloud Gateway are affected by this vulnerability.

Recommendations

It is recommended to change the default handling carriage returns and line feed configuration of the Cisco Secure Email Cloud Gateway and Cisco Secure Email Gateway to `Allow` [2] and not `Clean`.

References

[1] https://sec-consult.com/blog/detail/smtp-smuggling-spoofing-e-mails-worldwide/

[2] https://www.cisco.com/c/en/us/td/docs/security/esa/esa15-0/user_guide/b_ESA_Admin_Guide_15-0/b_ESA_Admin_Guide_12_1_chapter_0100.html?bookSearch=true#task_1254814__table_985308C400C84CE3BC190BC8A3A95D86