Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

SMTP Smuggling Enabling Spoofed Emails to Evade Authentication Protocols

Date of Publication	Admiralty Code	TA Number
January 4, 2024	A1	TA2024004

Summary

First appeared: June 7, 2023
Attack Region: Worldwide
Attack: A new email spoofing technique called "SMTP Smuggling" lets attackers send emails from fake addresses, bypassing security checks. This trick works by abusing how different servers handle line endings in email messages. The attack could affect millions of email users, so updating your software is crucial.

Attack Regions

Attack Details

#1 A new email spoofing technique known as "SMTP Smuggling" enables attackers to send emails from any address, evading traditional email authentication methods like SPF. This exploit capitalizes on vulnerabilities in how various email servers handle line endings in the SMTP protocol.

#2 SMTP, a TCP/IP protocol crucial to email communication, establishes connections between clients and servers for message transmission. There are two types of SMTP smuggling, outbound and inbound. These smuggling allows attackers to spoof the sender address on emails they originate.

#3 The vulnerability stems from inconsistencies in how outbound and inbound SMTP servers handle end-of-data sequences, empowering attackers to break out of message data, execute arbitrary SMTP commands, and send separate emails.

#4 Potentially, millions of domains and receiving servers worldwide were susceptible to this attack. This technique undermines email authenticity checks, including DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting, and Conformance (DMARC), and Sender Policy Framework (SPF).

#5 The potential for targeted phishing attacks is significant, as threat actors can impersonate legitimate senders and bypass established security protocols, presenting a notable cybersecurity risk. Organizations are advised to address vulnerabilities, conduct regular security testing, and enhance awareness training to mitigate the impact of SMTP smuggling.

Recommendations

Security Configuration Review: Perform a thorough review of the security configurations on your email servers, particularly focusing on default settings. Modify configurations to enhance security, following best practices recommended by the server vendors.

Email Security: Deploy robust email filtering solutions to detect and block malicious attachments and phishing attempts. Implement email mechanisms (SPF, DKIM, DMARC) to prevent email spoofing and phishing.

Patch and Update Software: Regularly update and patch all email servers and associated software. Ensure that you are using the latest versions to benefit from security improvements and fixes. Vendors, especially those identified with vulnerabilities, should be prompt in addressing and releasing patches.

Implement Strict Protocol Handling: Configure your SMTP servers to strictly adhere to the defined protocol specifications. Ensure that the servers handle end-of-data sequences consistently and accurately. By following protocol standards, the likelihood of exploitation decreases.

Validate "CR and LF Handling" Settings: Organizations should adjust the default settings related to "CR and LF Handling" in their SMTP servers. Change the configuration to less permissive to avoid these attacks.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0001 Initial Access	TA0005 Defense Evasion	T1566 Phishing
T1036 Masquerading	T1071 Application Layer Protocol	T1102 Web Service	T1659 Content Injection

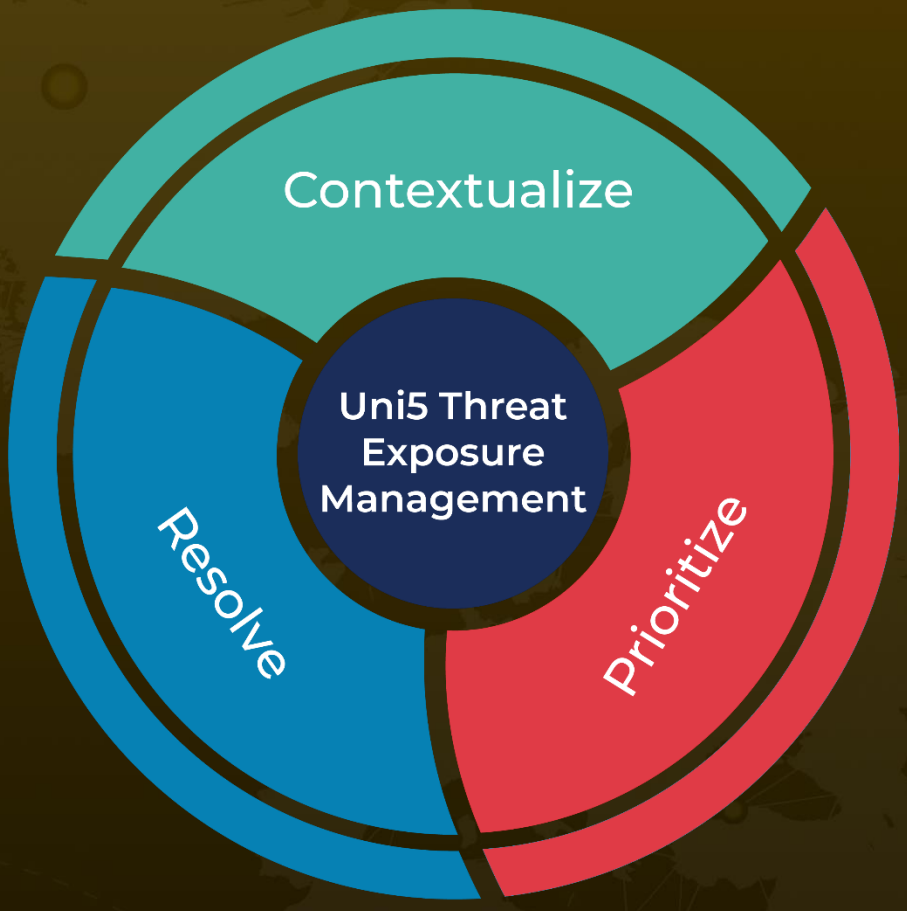
References

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 4, 2023 • 5:00 AM

© 2023 All Rights are Reserved by Hive Pro®

More at www.hivepro.com