

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

**Active! Mail Under Attack via CVE-2025-42599**

Date of Publication

April 24, 2025

Admiralty Code

A1

TA Number

TA2025123






# Summary

**First Seen:** April 2025

**Affected Products:** Qualitia Active! mail

**Impact:** A critical flaw in Active! mail, a web-based email client from QUALITIA CO., LTD., is actively being exploited, putting school and enterprise mail servers at serious risk. Tracked as CVE-2025-42599, the vulnerability is caused by a stack-based buffer overflow, which could allow unauthenticated remote attackers to execute arbitrary code or crash systems via specially crafted requests. With confirmed exploitation underway, users are strongly urged to update to latest version without delay to stay protected.

## CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-42599	Qualitia Active! Mail Stack Buffer Overflow Vulnerability	Qualitia Active! mail			

# Vulnerability Details

#1

A critical security flaw CVE-2025-42599 has been discovered in Active! mail, a web-based email platform developed by QUALITIA. Widely used in corporate and educational environments, this email client allows users to access their inbox directly through a browser, making it a convenient and lightweight alternative to traditional desktop email programs.



#2

The vulnerability is a stack-based buffer overflow, which can be triggered by a maliciously crafted request from a remote attacker even without authentication. If successfully exploited, it could allow the attacker to execute arbitrary code on the server or crash the system entirely, leading to a denial-of-service (DoS) scenario.

#3

The vulnerability is already being actively exploited, users are strongly urged to upgrade to Active! mail version 6 (BuildInfo: 6.60.06008562) as soon as possible to protect their systems from potential compromise.

## Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-42599	Active! mail 6 BuildInfo: 6.60.05008561 and earlier	cpe:2.3:a:qualitia:active_mail:*:*:*:*:*	CWE-121

## Recommendations



**Update:** Upgrade to Active! mail version 6 (BuildInfo: 6.60.06008562) or a newer release right away. This update patches a serious flaw that could let attackers take control of your system or crash it remotely.



**Restrict External Access:** To reduce risk, keep the Active! mail interface behind a firewall or VPN. Avoid making it directly accessible from the internet unless there’s a strong, justified need. Limiting exposure helps block attackers from easily reaching vulnerable systems.





**Monitor and Scan for Threats:** Enable logging and continuous monitoring on mail servers to catch any suspicious activity, such as unusual requests or signs of exploitation like denial-of-service or remote code execution attempts. Additionally, run regular vulnerability scans to detect outdated or unpatched instances of Active! mail across your environment, ensuring swift remediation before attackers can take advantage.



**Back Up Email Data:** Make sure to routinely back up all user email data so you can quickly recover in case of a system compromise or crash caused by a denial-of-service (DoS) attack. Reliable backups can significantly reduce downtime and data loss during an incident.



**Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third party vendors, especially for critical applications and services.



## Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0040</u></b> Impact
<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1059</u></b> Command and Scripting Interpreter
<b><u>T1499</u></b> Endpoint Denial of Service			



## Patch Details

To address this critical vulnerability, QUALITIA has released a patched version of Active! mail: version 6 (BuildInfo: 6.60.06008562).

Link: <https://jvn.jp/en/jp/JVN22348866/>





# References

<https://jvn.jp/en/ip/JVN22348866/>

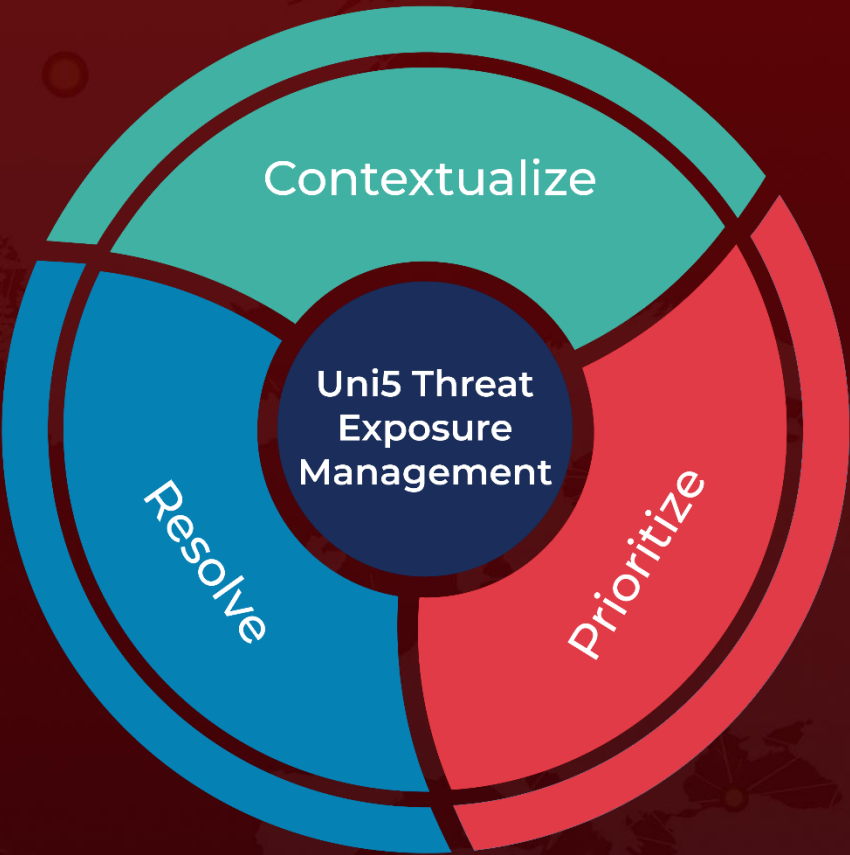
[https://www.qualitia.com/ip/news/2025/04/18\\_1030.html](https://www.qualitia.com/ip/news/2025/04/18_1030.html)



# 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  
**April 23, 2025 • 4:40 AM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)