Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Exim Vulnerable to Zero-Day Remote Code Execution Attacks

Date of Publication	Admiralty Code	TA Number
October 3, 2023	A1	TA2023394

Summary

First Seen: September 27, 2023
Affected Products: Exim
Affected Platform: Unix
Impact: Six zero-day vulnerabilities have been discovered in the Exim Internet Mailer, potentially putting thousands of email servers worldwide at risk. These vulnerabilities, if successfully exploited, could result in information disclosure and remote code execution, posing significant security threats to affected systems. Among these vulnerabilities, CVE-2023-42115 stands out as the most severe, as it allows remote, unauthenticated attackers to execute arbitrary code on Exim installations.

⚙ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-42114	Exim Information Disclosure Vulnerability	Exim	✓	✗	✓
CVE-2023-42115	Exim Remote Code Execution Vulnerability	Exim	✓	✗	✓
CVE-2023-42116	Exim Buffer Overflow Remote Code Execution Vulnerability	Exim	✓	✗	✓
CVE-2023-42117	Exim Remote Code Execution Vulnerability	Exim	✓	✗	✗
CVE-2023-42118	Exim Remote Code Execution Vulnerability	Exim	✓	✗	✗
CVE-2023-42119	Exim Information Disclosure Vulnerability	Exim	✓	✗	✗

Vulnerability Details

#1

Numerous security vulnerabilities have recently been revealed in the Exim Internet Mailer, posing a potential risk to thousands of email servers worldwide. Among these vulnerabilities, a critical zero-day vulnerability, denoted as CVE-2023-42115, has been identified in all versions of the Exim mail transfer agent (MTA) software. This specific vulnerability has the capacity to enable unauthenticated attackers to achieve remote code execution (RCE) on Internet-facing servers that utilize Exim.

#2

This vulnerability resides in the SMTP service, which typically listens on TCP port 25 by default. It arises from a boundary error that occurs during the processing of the AUTH command. An attacker, without needing authentication, can send carefully crafted data to the server, triggering an out-of-bounds write operation. The vulnerability results from inadequate validation of user-supplied data, which can lead to data being written beyond the buffer's boundaries. Exploiting this flaw empowers the attacker to execute code within the context of the service account.

#3

Both CVE-2023-42114 and CVE-2023-42116 result from inadequate validation of user-supplied data and impact systems using SPA/NTLM. Fixes for CVE-2023-42114, CVE-2023-42115, and CVE-2023-42116 is provided with version 4.96.1.

#4

The fix for the other three CVEs is not yet incorporated in version 4.96.1. CVE-2023-42117 is a memory corruption vulnerability, which can be mitigated by utilizing a trusted proxy-protocol proxy. CVE-2023-42118 affects the SPF subsystem and can be mitigated by avoiding 'spf' conditions in ACL. CVE-2023-42119 can be exploited through DNS lookups, and using a trustworthy DNS resolver will aid in mitigating this vulnerability.

#5

An attacker could potentially exploit these vulnerabilities in conjunction with other security flaws, resulting in information disclosure and the execution of arbitrary code within the context of the service account.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-42114	Exim: 4.96 or earlier versions	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*	CWE-125
CVE-2023-42115	Exim: 4.96 or earlier versions	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*	CWE-787
CVE-2023-42116	Exim: 4.96 or earlier versions	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*	CWE-121
CVE-2023-42117	Exim: 4.96 or earlier versions	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*	CWE-119
CVE-2023-42118	Exim: 4.96 or earlier versions	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*	CWE-191
CVE-2023-42119	Exim: 4.96 or earlier versions	cpe:2.3:a:exim:exim:4.96:*:*:*:*:*:*	CWE-125

Recommendations

Apply Patch: Install the security patch provided by Exim to address the CVE-2023-42114, CVE-2023-42115 and CVE-2023-42116 vulnerabilities. These patches shall close the security gap that allows attackers to exploit the vulnerability.

Least Privilege Principle: Limit user and system accounts to the minimum level of access required to perform their tasks. Avoid running services with root or administrator privileges whenever possible.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0042 Resource Development	T1190 Exploit Public-Facing Application	T1078 Valid Accounts
T1588 Obtain Capabilities	T1588.006 Vulnerabilities		

Patch Details

It is recommended to update the latest version of Exim to 4.96.1 which addresses the CVE-2023-42114, CVE-2023-42115 and CVE-2023-42116 vulnerabilities. Also, refer to Exim link for information on mitigation strategies for the other three unfixed vulnerabilities.

Patch Link:
https://exim.org/

Mitigation Details:
https://exim.org/static/doc/security/CVE-2023-zdi.txt

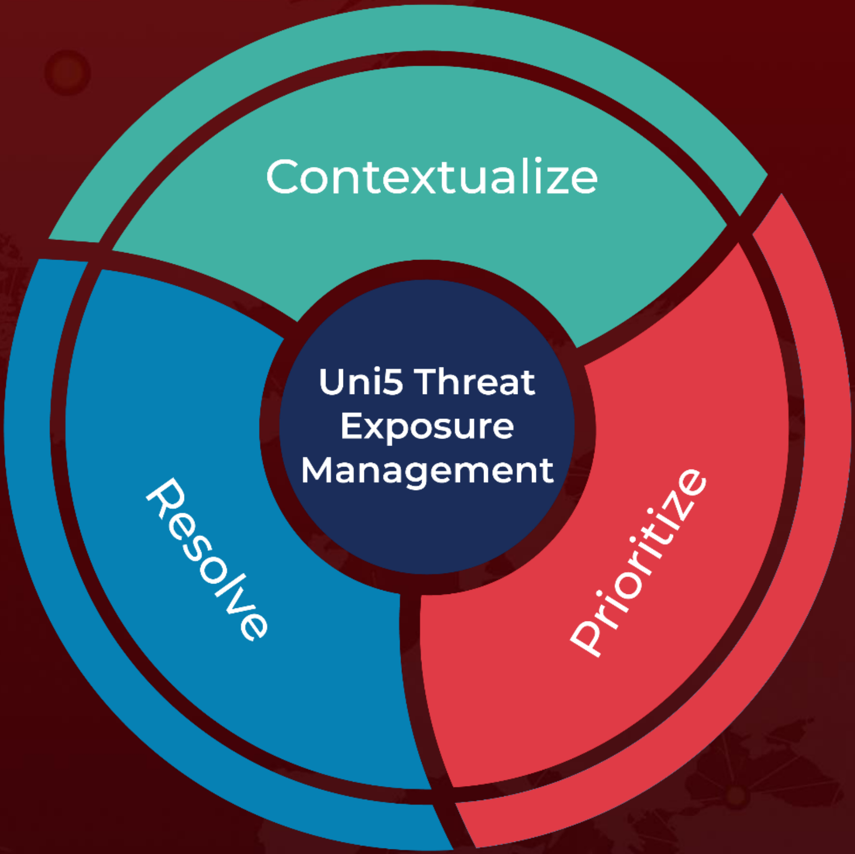
References

https://exim.org/static/doc/security/CVE-2023-zdi.txt

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

October 3, 2023 • 7:40 AM

More at www.hivepro.com