Multiple Vulnerabilities in Zimbra

Severity Level: Medium

Components Affected

- Zimbra Collaboration Joule prior to 8.8.15 Patch 45 GA
- Zimbra Collaboration Kepler prior to 9.0.0 Patch 38 GA
- Zimbra Collaboration Daffodil prior to 10.0.6

Overview

Multiple vulnerabilities were identified in Zimbra, where a remote attacker could exploit some of these vulnerabilities to trigger cross-site scripting, security restriction bypass, data manipulation and sensitive information disclosure on the targeted system.

Description

Multiple vulnerabilities have been discovered in the Zimbra collaboration platform, posing a significant security risk. If exploited by a remote attacker, these vulnerabilities could lead to a range of critical consequences, including the execution of malicious scripts through cross-site scripting (XSS), bypassing security restrictions to gain unauthorized access, manipulating data within the system, and disclosing sensitive information. The potential impact of these vulnerabilities encompasses unauthorized actions, data theft, session hijacking, and exposure of confidential information.

Impact

- Information Disclosure
- Data Manipulation
- Cross-Site Scripting
- Security Restriction Bypass

Solution/ Workarounds

Before installation of the software, please visit the software vendor web-site for more details.

Apply fixes issued by the vendor:

- https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P45
- https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P38
- https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.6

Reference

https://www.hkcert.org/security-bulletin/zimbra-multiple-vulnerabilities_20231219

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.