CYBER DEFENSE AFRICA: SECURITY ANNOUNCEMENT **Date**: 12/08/2022

Content Type	Description
Title	*Critical vulnerabilities in the Zimbra mail service*
Id	*202208/Alert/05*
Code LTP	*White*
Risk Level	*High*
Affected Application and Service	*N/A*
Version	*Version less than 8.8.15 p31.1, 9.0.0 p24.1 for CVE-2022-27925* *Version less than 8.8.15 p32 and 9.0.0 P26 For CVE-2022-37042*
Platform	*Zimbra*
Update	*Zimbra version 8.8.15 p33 and 9.0.0 p26*
Summary	*Vulnerability Allowing Attackers to Steal Plaintext Credentials of Users of Targeted Zimbra Instances*
Impacts	- *Access to victims' mailboxes* - *Privilege escalation and access to other internal services* - *Access tox sensitive informations* - *Sendingphishing messages to the user's contacts*
Detailed Description	*CVE-2022-27924 is a command injection flaw in the platform that could lead to arbitrary Menchahed command execution and theft of sensitive information. This is possible by poisoning the IMAP route cache entries in the Memcached server that is used to find Zimbra users and forward their HTTP requests to the appropriate back-end services. Memcached is a key-value storage system in memory used as a high-performance cache or session store for external databases and API calls – in this case, the search service.* *CVE-2022-37042 affects authentication bypass in MailBoxImportServlet*
Solutions	*The Zimbra platform advises to update to the latest patch available on their site if the versionin use is earlier than version 8.8.15 P33 and 9.0.0 P26*
Links for more details	*https://blog.sonarsource.com/zimbra-mail-stealing-clear-text-credentials-via-memcache-injection/*