Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 153 **20-06-2022**

Name: Windows Memcached poisoning with unauthenticated request **(CVE-2022-27924)**

Threat Classification: Memcached Poisoning with Unauthenticated Request

Affected Versions: Zimbra Collaboration (aka ZCS) 8.8.15 and 9.0

Summary:

Zimbra Collaboration (ZCS) allows an unauthenticated attacker to inject arbitrary memcache commands into a targeted instance. These memcache commands becomes unescaped, causing an overwrite of arbitrary cached entries.

If successfully exploited, it enables an unauthenticated attacker to steal clear text passwords of user's sans any user interaction. With the consequent access to the victims' mailboxes, attackers can potentially escalate their access to targeted organizations and gain access to various internal services and steal highly sensitive information.

For the latest release and patches, please be sure to update your Zimbra Collaboration servers with the software available on our Download pages:

- Network Edition: https://www.zimbra.com/downloads/ne-downloads.html
- Open-Source Edition: https://www.zimbra.com/downloads/os-downloads.html

Severity	**High**
Attack Vector	**Network**
CVS Score	**7.5**

Recommendations:

- Please visit the website link and check **mitigations** and **workarounds** for the aforementioned vulnerabilities: It is recommended to update the current versions to the patched version by the link below:

  Network Edition: https://www.zimbra.com/downloads/ne-downloads.html

  Open-Source Edition: https://www.zimbra.com/downloads/os-downloads.html

- It is recommended to use encryption techniques for password protection.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- Designate a PoC from your security / Network team (if yet not designated), for seeking assistance and reporting security issues.