Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 157 **25-11-2022**

Name: Zimbra Zero-Day Vulnerability (CVE-2022-41352)

Threat Classification: Remote Code Execution, Arbitrary File Upload

Affected Versions:

- Zimbra Collaboration (ZCS) 8.8.15 and 9.0

Summary:

An issue was discovered in Zimbra Collaboration (ZCS) 8.8.15 and 9.0. The vulnerability affects a component of the Zimbra suite called Amavis, and more specifically the cpio utility it uses to extract archives. An attacker can upload arbitrary files through amavisd via a cpio loophole that can lead to incorrect access to any other user accounts. The underlying cause is another vulnerability (CVE-2015-1197) in cpio. Inexplicably, distribution maintainers appear to have reverted the patch and use a vulnerable version instead. This creates a large attack surface where any software relying on cpio might in theory be leveraged to take over the system. CVE-2015-1197 is a directory traversal vulnerability: extracting specially crafted archives containing symbolic links can cause files to be placed at an arbitrary location in the file system.

Severity	**Critical**
Attack Vector	**Network**
Privileges required	**None**

Zimbra recommends pax over cpio. Also, pax is in the prerequisites of Zimbra on Ubuntu; however, pax is no longer part of a default Red Hat installation after RHEL 6 (or CentOS 6). Once pax is installed, amavisd automatically prefers it over cpio.

The exploitation scenario unfolds as follows:

- An attacker sends an e-mail with a malicious tar archive attached.
- Upon receiving the email, Zimbra submits it to Amavis for spam and malware inspection.
- Amavis analyzes the email attachments and inspects the contents of the attached archive. It invokes cpio and CVE-2015-1197 is triggered.
- During the extraction, a JSP webshell is deployed on one of the public directories used by the webmail component. The attacker can browse to the webshell to start executing arbitrary commands on the victim machine.

Recommendations:

- Please visit the following link for Zimbra released patch along with installation instructions, moreover, it is recommended to install the newest updates/patches from the following link:

  https://wiki.zimbra.com/wiki/Zimbra_Releases

- It is recommended to immediately upgrade to secure versions 5.3.18 or 5.2.20.
- Do not download attachments from emails unless they are from a trusted source.
- Regularly provide Cyber security awareness training to the employees.
- In case of any incident, please report to this office.