**Alert – Simple Mail Transfer Protocol (SMTP) Open Relay Vulnerability**

**Description**

An open mail relay is an SMTP server configured on port 25 in such a way that it allows anyone on the Internet to send email through it, not just mail destined to or originating from known users. By processing mail that is neither for nor from a local user, an open relay makes it possible for an unscrupulous sender to route large volumes of spam. In effect, the owner of the server, who is typically unaware of the problem, donates network and computer resources to the sender's purpose of only instilling fear to receivers but without any system damage.

This vulnerability in the SMTP open relay connection could allow abuse by spammers which means that an unauthenticated, remote attacker could send unsolicited email messages, aka a Mail Relay Vulnerability. In this case, the sender address can be the same as the recipient address. The spammer is sending an email to a user on his server. The vulnerability is due to misconfiguration of mail and improper handling of domain information in the affected software which allows an unauthenticated, remote attacker to be able to exploit this vulnerability by sending crafted requests to the targeted application. A successful exploit could allow the attacker to send email messages to arbitrary addresses. (CVE-2006-5545) (CVE-2006-0977) (CVE-2005-2857) (CVE-2002-0054) (CVE-1999-0512) (CVE-1999-0682)

Microsoft has classified this vulnerability as being a “spammable or spoofable (susceptible to spamming, spoofing or phishing)” exploit. This means that a remote attacker exploiting this vulnerability can spread a phishing emails to the users and spoof his emails to look like they are coming from himself.

**Vulnerable or affected systems:** All Microsoft Exchange Servers versions prior to 2016

**Solution:**

**Recommendation:**

- We are recommend every user who received or will receive these emails to report immediately to mail server administrator and ignore what attacker is requesting,
- Do not pay the ransom they are requesting
- Change your credentials regularly and apply password complex policy

**Mitigation:**

1. **Apply DKIM policy where it is possible**
2. **Enable anti-spamming, anti-malware and anti-spoofing on mail server**
3. **Apply SPF and DMARC where it is possible**

| |
|---|
| **Affected users should**: contact RW-CSIRT: Call **4045** or write to **security@risa.rw** to help for analyzing the source of the incident and help to apply recommendation. |
| **National Computer Security and Incident Response Team (Rw-CSIRT) Mission** |
| Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of “early **Detection**, **Prevention**, **Response** to incidents and **Reduce** Vulnerability” and raise cyber security awareness in public. |