UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00213

MOZILLA THUNDERBIRD EMAIL CLIENT VULNERABILITY

DATE ISSUED: 18th October 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

It has been discovered that Mozilla's email client software Thunderbird is host to several vulnerabilities, the most severe of which could allow Remote Code Execution (RCE). Depending on the level of the user's access privileges, this could lead to full device takeover.

BREAKDOWN

While there are no reports of these vulnerabilities under exploit in the wild, an attacker who gains access to a privileged (administrator) user account through compromising the email client could have the ability to install and remove programs, view, change or delete data, and add new accounts with full access privileges. These vulnerabilities affect all versions of Thunderbird prior to 91.2. The two that could lead to RCE are being tracked as CVE-2021-38500 and CVE-2021-38501. A Man in the Middle allowing a malicious actor to hijack an authenticated session an execute SMTP commands in a downgrade attack is tracked under CVE-2021-38502. Further vulnerabilities that could lead to memory corruption are CVE-2021-38496 and CVE-2021-38498, a memory leak CVE-2021-32810 and a spoofing attack CVE-2021-32810.

REMEDIATION STEPS

- Update to the latest version of Mozilla Thunderbird after testing has been completed
- Check user access privileges and alter these to correspond to their required level of access – only run as administrator where absolutely necessary. Apply the principles of least privilege.
- Educate users on the dangers of social engineering (phishing) emails and visiting untrusted sites.

REFERENCES & RESOURCES

Mozilla https://www.mozilla.org/en-US/security/advisories/mfsa2021-47/
CIS Advisory