

USN-4736-1: Thunderbird vulnerabilities

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, or execute arbitrary code. (CVE-2020-26976, CVE-2021-23953, CVE-2021-23954, CVE-2021-23960, CVE-2021-23964)

It was discovered that responses received during the plaintext phase of the STARTTLS connection setup were subsequently evaluated during the encrypted session. A person in the middle could potentially exploit this to perform a response injection attack. (CVE-2020-15685)