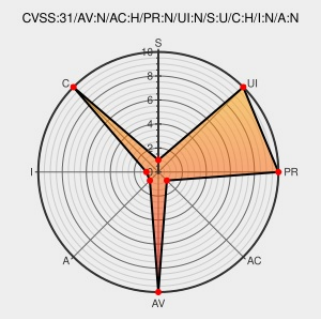
CVE-2020-15646

Published on: 10/08/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-15646

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Thunderbird from Mozilla contain the following vulnerability:

If an attacker intercepts Thunderbird's initial attempt to perform automatic account setup using the Microsoft Exchange autodiscovery mechanism, and the attacker sends a crafted response, then Thunderbird sends username and password over https to a server controlled by the attacker. This vulnerability affects Thunderbird < 68.10.0.

CVE-2020-15646 has been assigned by security@mozilla.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Mozilla** - **Thunderbird** version **< 68.10.0**

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link

Access Denied	Issue Tracking Permissions Required Vendor Advisory bugzilla.mozilla.org text/html	MISC bugzilla.mozilla.org/show_bug.cgi?id=1606610
Security Vulnerabilities fixed in Thunderbird 68.10.0 — Mozilla	Vendor Advisory www.mozilla.org text/html	MISC www.mozilla.org/security/advisories/mfsa2020-26/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→