CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-044

Remote Code Execution Vulnerability Affecting Microsoft Exchange

September 14, 2020 — v1.1

TLP:WHITE

History:

- *09/09/2020 — v1.0 – Initial publication*
- *14/09/2020 — v1.1 – Update to add PoC and details*

Summary

On 9th of September 2020, Microsoft released several security advisories, updates, and workarounds to address security vulnerabilities [1]. One of the reported vulnerabilities affects Microsoft Exchange server [2].

Based on the description provided by Microsoft, the vulnerability is due to improper validation of cmdlet arguments. An attacker authenticated with specific Exchange role could run arbitrary code in the context of the System user, leading to a full compromise of the Exchange server.

On the 10th of September 2020, Source Incite released details and proof-of-concept for the vulnerability [5]. The vulnerability is due to lack of proper validation of user-supplied data when using the `New-DlpPolicy` cmdlet. To exploit this vulnerability, the authenticated attacker needs the *Data Loss Prevention* (DLP) role assigned. This role is usually assigned to administrationa account only, however this type of vulnerabilities trigger high interest for different threat actors and proof-of-concept usually emerges quite quickly after the release of a patch. For this reason, it is highly recommended to patch the exposed Exchange servers as soon as possible.

Technical Details

The vulnerability was assigned *CVE-2020-16875* [4].

The vulnerability is a remote code execution in Microsoft Exchange server due to improper validation of `New-DlpPolicy` cmdlet arguments. To exploit the vulnerability, an attacker needs the *Data Loss Prevention* (DLP) role assigned to the used account.

To exploit the vulnerability, tha attacker needs to create a malicious dlp policy (XML format) by injecting a payload in the `commandBlock` sub-element of the `policyCommands` element of the new policy (stored in a `dlpPolicyTemplate` element) and call this created XML using the `New-DlpPolicy` cmdlet.

Products Affected

This vulnerability affects the following Microsoft Exchange Server versions:

- Microsoft Exchange Server 2019 before Cumulative Update 5
- Microsoft Exchange Server 2016 before Cumulative Update 16

Recommendations

CERT-EU recommends updating Microsoft Exchange Server following Microsoft guidance as soon as possible [3].

References

[1] https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Sep

[2] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-16875

[3] https://support.microsoft.com/en-us/help/4577352/security-update-for-exchange-server-2019-and-2016

[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16875

[5] https://srcincite.io/advisories/src-2020-0019/