CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-049

Critical Vulnerability in Microsoft Outlook

October 14, 2020 — v1.0

TLP:WHITE

History:

- *14/10/2020 — v1.0 – Initial publication*

Summary

On 13th of October 2020, Microsoft released several security advisories to address security vulnerabilities. One of the reported vulnerabilities, affects Oulook, and it can be triggered by previewing a malicious e-mail. An attacker who successfully exploits this vulnerability could gain the ability to execute code on the target client [1].

Technical Details

Exploitation of the vulnerability requires that a user opens a specially crafted file with an affected version of Microsoft Outlook software. In an e-mail attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an e-mail or instant message, and then convince them to open the specially crafted file.

The remote code execution vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory. An attacker who successfully exploits the vulnerability could run arbitrary code in the context of the System user [1]. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights [1].

This vulnerability was reported through the ZDI program. The specific flaw exists within the parsing of HTML content in an email. The issue results from the lack of proper validation of the length of user-supplied data before copying it to a fixed-length heap-based buffer [2].

Affected Products

Microsoft Outlook 2016, Microsoft Outlook 2019 and Microsoft 365 Apps for Enterprise [1].

Recommendations

Apply the patches [1].

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

References

[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16947

[2] https://www.zerodayinitiative.com/blog/2020/10/13/the-october-2020-security-update-review