CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-010

Microsoft Exchange Server – Remote Code Execution Vulnerability

February 26, 2020 — v1.0

TLP:WHITE

History:

- *26/02/2020 — v1.0 – Initial publication*

Summary

Microsoft released a fix for a remote code execution vulnerability in Microsoft Exchange (CVE-2020-0688) [1]. The vulnerability exists because Exchange fails to create unique cryptographic keys at installation time, leading to all Exchange servers using the same `validationKey` and `decryptionKey` values.

Knowledge of a the validation key allows an authenticated user with a mailbox on the server to pass arbitrary objects to be deserialized by the web application. That runs as `SYSTEM`, leading to remote code execution with the highest privileges.

On February 25th 2020, Zero Day Initiative released a blog post detailing how to exploit the vulnerability [2]. Any user with an account on an Exchange server can easily exploit the remote code execution vulnerability.

Some researchers point-out that scanning for vulnerable Exchange servers is ongoing [3].

Technical Details

A remote code execution vulnerability exists in Microsoft Exchange due to improper generation of validation and decryption keys during installation.

To exploit this vulnerability, an attacker would need to authenticate to a Microsoft Exchange Server with a valid account (via Outlook Web Access for example) and extract some parameters from the communication with the server:

- `ViewStateUserKey` and `__VIEWSTATEGENERATOR` from the response of a request sent to `/ecp/default.aspx`,
- `ASP.NET_SessionId` in the request headers,
- `validationKey` which is always the same for all vulnerable Exchange servers.

The attacker can then generate a malicious URL by serializing and URL-encoding a payload using the gathered information. Submitting the URL will trigger a `500 Unexpected Error` but the crafted payload will be executed on the server with `SYSTEM` rights.

Products Affected

- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

Recommendations

Apply February 2020 security updates as described by Microsoft advisory [1].

Check the validation key value on Microsoft Exchange Servers in `web.config`. If the value is equal to `CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BF`, the server is vulnerable

References

[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0688

[2] https://www.thezdi.com/blog/2020/2/24/cve-2020-0688-remote-code-execution-on-microsoft-exchange-server-through-fixed-cryptographic-keys

[3] https://twitter.com/bad_packets/status/1232428319733272579