SECURITY
MADEIN.LU
circl.lu cases.lu c3.lu

INFO

[18.03.2021]

Exploitation of vulnerabilities in Microsoft Exchange

Several critical vulnerabilities have been discovered in the unpatched Microsoft Exchange 2010, 2013, 2016 and 2019 servers (Exchange Online servers are not affected). The exploitation of these security breaches leads to a risk of data theft or destruction and infrastructure compromise for the impacted companies.

These vulnerabilities were previously exploited by a group of activities - named HAFNIUM by Microsoft, since late 2020. Once these vulnerabilities became public in early March, their exploitation intensified, including the deployment of the new "*DearCry*" ransomware and cryptocurrency mining malware.

The situation is alarming due to the number of potentially affected servers in the world. In Luxembourg, a significant number of Microsoft Exchange servers are considered vulnerable.

CIRCL (Computer Incident Response Center Luxembourg), the cyber incident emergency response team for the private sector, municipalities and non-governmental entities in Luxembourg, has the objective of helping the component entities of the Luxembourg economy when the security of their IT systems is at risk.

CIRCL experts can assist all potentially affected companies and organisations individually in the process of detecting and resolving possible intrusions.

A Technical Report (TR-61) that includes all recommendations for fixing and mitigating potential bugs and risks has been issued. In this report, it is recommended, to this day, to consider any unpatched Microsoft Exchange server as compromised and to follow the following procedure (see next page):

Released by SECURITYMADEIN.LU

- Prioritize installing updates on Microsoft Exchange servers, deployed by Microsoft. All affected Exchange Servers should ultimately be updated.
- However, CIRCL warns that relying on patching is not sufficient. These patches will not secure already compromised servers, as some of them were already exploited before the patch deployment. Criminals may have already installed backdoors. It is recommended to scan the potentially compromised Microsoft Exchange server with a script like:
    - https://github.com/microsoft/CSS-Exchange/tree/main/Security
    - https://github.com/cert-lv/exchange_webshell_detection
- Finally, it is strongly recommended to review the security and especially the logs of the Microsoft Exchange server for any indicators of exploitation as well as to apply standard incident response procedures.

The specific indicators of compromise (IoC) are also available in various MISP sharing communities (MISP event uuid: fd875781-262e-4159-a0cd-ac0241784cc7). Access request here.

Exploitation risks that can be accentuated by vulnerabilities in the Microsoft DNS server:

On March 10, 2021, CERT-EU published a security advisory (2021-014) reporting 5 vulnerabilities (one of which is considered critical by Microsoft, CVE-2021-26897) in Windows servers 2016, 2019, 2012 (R2 included), 2008 (R2, R2 SP1 and R2 SP2 included), version 2004, version 1909 and version 20H2. To be exploitable, the server must have the DNS role enabled and dynamic update enabled (default configuration).

Although there is no evidence of ongoing exploitation of these vulnerabilities yet, it is recommended to apply the patches as soon as possible and to prioritise the updates on Internet-facing Windows DNS Servers.
Two mitigating measures can be taken to limit the exploitability of the vulnerabilities:

- disable the Dynamic Update feature
- enable secure zone updates

However, enabling secure zone updates protects against attacks on public interfaces, but not against a criminal who already has a foothold in the network (computer linked to a domain), which increases the risks induced by vulnerabilities in some Microsoft Exchange servers.

If you have any questions regarding this situation, please do not hesitate to contact:

- your IT department, to make sure that all necessary updates and scans have been performed
- your IT Integrator
- your Microsoft support or check the following Microsoft manual: One-Click Microsoft Exchange On-Premises Mitigation Tool
- CIRCL :

circl.lu
Computer Incident
Response Center
LUXEMBOURG

- **Phone** : (+352) 247 88444
- **E-mail** : info@circl.lu

About SECURITYMADEIN.LU

SECURITYMADEIN.LU is the Cybersecurity Agency for the Luxembourg Economy and Municipalities.

The agency contributes and supports the continued reliability to the Luxembourg economy's trustworthiness by providing extensive cybersecurity expertise and solutions through its 3 departments: CIRCL (Computer Incident Response Center Luxembourg), CASES (Cyberworld Awareness Security Enhancement Services – Luxembourg) and C3 (Cybersecurity Competence Center – Luxembourg).

www.securitymadein.lu
www.cases.lu
www.circl.lu
www.c3.lu

Released by SECURITYMADEIN.LU