EUROPEAN UNION AGENCY
FOR CYBERSECURITY

MICROSOFT EXCHANGE VULNERABILITIES

Situation update and mitigation

MARCH 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use sat@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Operational Cooperation Unit – Situational Awareness Team

LEGAL NOTICE

COPYRIGHT NOTICE

TABLE OF CONTENTS

1. INTRODUCTION

On 2nd March 2021, Microsoft released security updates for Microsoft Exchange server suite. Active exploitation has been observed ever since on premises running MS Exchange installations. Although the initial focus of malicious attacks was observed mainly in the US, incidents rapidly expanded around the globe, including in the EU by an increasing number of hacking groups.

In the EU, an increasing number of MS Exchange installations have also been found to be the target of malicious attacks. Although the initial focus of attacks was on exfiltration of information, attackers seem to be exploiting the MS exchange vulnerabilities to plant ransomware in order to gain profits. Cases of such systems infected with the DearCry ransomware have been reported.

On 7th March 2021, the European Banking Authority (EBA) published a statement on their website announcing that their Microsoft Exchange servers had been the victim of a cyber-attack, as a result of the recently-disclosed zero-day vulnerabilities in the servers[1]. The incident has been mitigated according to a later statement by EBA, without affecting confidentiality of EBA systems and data[2].

The EU Cyber Crises Liaison Organisation Network (CyCLONe) and the EU CSIRTs network are monitoring the situation and collecting information.

2. SITUATION UPDATE[3]

Scans conducted by researchers indicate that on March 5th there were around 250,000 vulnerable servers. That number dropped to around 60,000 over the next 10 days. The initial rush to patch by companies with good security posture has considerably lowered the number of vulnerable systems exposed.

There are indications that threat actors are targeting Exchange Servers from infrastructure hosted in a number of EU countries, Hong Kong, United States, Belize, Japan, and Singapore. Wide scanning activities for the vulnerabilities have been observed from systems in the EU, the United States, Hong Kong and China.

Botnet operators are likely to be leveraging the vulnerabilities to expand their operations. The LemonDuck botnet has been observed exploiting the vulnerabilities recently.

Ransomware operators are also leveraging the vulnerabilities and it is likely that this activity will continue. The new DearCry ransomware has been deployed following successful exploitation with victims observed in some EU countries, Indonesia, India and the United States.

[1] https://www.eba.europa.eu/cyber-attack-european-banking-authority
[2] https://www.eba.europa.eu/cyber-attack-european-banking-authority-update-3
[3] Source: ENISA trusted partners

3. ASSESSMENT

This threat is categorised as severe due to active exploitation in the wild and the popularity and widespread utilisation of MS exchange server products.

The first observed APT group to have exploited the vulnerabilities has been the “Hafnium” cyberespionage group, which targets primarily entities in the United States across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defence contractors, policy think tanks, and NGOs. In the meantime, several other APT groups and threat actors have used the vulnerabilities to exfiltrate data and spread malware in the EU and across the world.

4. ADVICE AND MITIGATION

MS Exchange vulnerabilities once exploited may lead to network compromise, data exfiltration and ransomware attacks. Senior management of public and private organisations and companies should consider these types of attacks probable and of a high risk. Appropriate aid should be allocated for detection and removal from 3rd parties if they do not possess the necessary capacities to deal with this threat.

The vulnerabilities being exploited are:

- CVE-2021-26855, a server-side request forgery (SSRF) vulnerability in Microsoft Exchange that could be exploited by an attacker to authenticate as the Exchange server by sending arbitrary HTTP requests

- CVE-2021-26857, an insecure deserialization issue that resides in the Unified Messaging service. This flaw allows an attacker with administrative permission to run code as SYSTEM – the highest privilege level – on the Exchange server.

- CVE-2021-26858 and CVE-2021-27065, both of which allow authenticated users to arbitrarily write files to the Exchange Server

The combination of a vulnerability that allows unauthorised actors to authenticate and several vulnerabilities that allow arbitrary write access to authenticated users is what makes these vulnerabilities very dangerous.

Organisations using affected Microsoft Exchange versions are recommended to patch the flaws immediately and examine their systems for indicators of compromise[4]. Microsoft is continuously updating its relative advisories and has published relative guidance and a mitigation tool[5].

Additional technical information and advice is provided by CERT-EU technical advisory[6]

[4] https://github.com/microsoft/CSS-Exchange/tree/main/Security
[5] https://msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/
[6] https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-013.pdf

Attack patterns and detection routines for vulnerable systems have been incorporated into the security research tools “metasploit” and “nmap” respectively.

Due to the high probabilities of attackers having attempted to gain persistence and performed lateral movement, any infrastructure with vulnerable Exchange servers should be carefully monitored for additional compromised systems.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu