Exploitation of the CVE-2021-40444 vulnerability in MSHTML

16 SEP 2021 2 minute read

Table of Contents

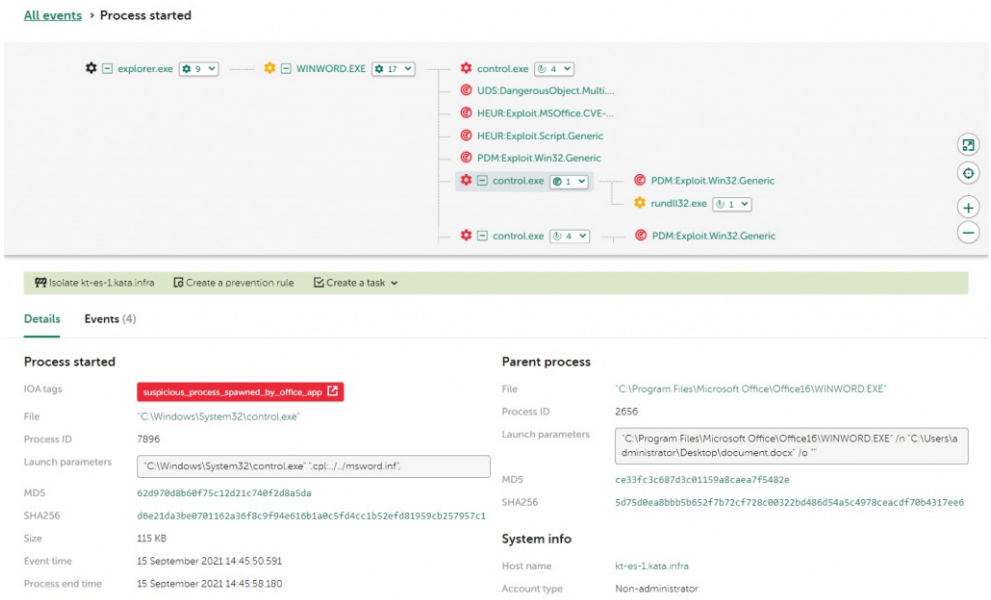
Summary

Last week, Microsoft reported the remote code execution vulnerability CVE-2021-40444 in the MSHTML browser engine. According to the company, this vulnerability has already been used in targeted attacks against Microsoft Office users. In attempt to exploit this vulnerability, attackers create a document with a specially-crafted object. If a user opens the document, MS Office will download and execute a malicious script.
According to our data, the same attacks are still happening all over the world. We are currently seeing attempts to exploit the CVE-2021-40444 vulnerability targeting companies in the research and development sector, the energy sector and large industrial sectors, banking and medical technology development sectors, as well as telecommunications and the IT sector. Due to its ease of exploitation and the few published Proof-of-Concept (PoC), we expect to see an increase in attacks using this vulnerability.

Geography of CVE-2021-40444 exploitation attempts

Kaspersky is aware of targeted attacks using CVE-2021-40444, and our products protect against attacks leveraging the vulnerability. Possible detection names are:

- HEUR:Exploit.MSOffice.CVE-2021-40444.a
- HEUR:Trojan.MSOffice.Agent.gen
- PDM:Exploit.Win32.Generic



Killchain generated by KEDR during execution of CVE-2021-40444 Proof-of-Concept

Experts at Kaspersky are monitoring the situation closely and improving mechanisms to detect this vulnerability using Behavior Detection and Exploit Prevention components. Within our Managed Detection and Response service, our SOC experts are able to detect when this vulnerability is expoited, investigate such attacks and notify customers.

Technical details

The remote code execution vulnerability CVE-2021-40444 was found in MSHTML, the Internet Explorer browser engine which is a component of modern Windows systems, both user and server. Moreover, the engine is often used by other programs to work with web content (e.g. MS Word or MS PowerPoint).
In order to exploit the vulnerability, attackers embed a special object in a Microsoft Office document containing an URL for a malicious script. If a victim opens the document, Microsoft Office will download the malicious script from the URL and run it using the MSHTML engine. Then the script can use ActiveX controls to perform malicious actions on the victim's computer. For example, the original zero-day exploit which was used in targeted attacks at the time of detection used ActiveX controls to download and execute a Cobalt Strike payload. We are currently seeing various types of malware, mostly backdoors, which are delivered by exploiting the CVE-2021-40444 vulnerability.

Mitigations

- Follow Microsoft security update guidelines.
- Use the latest Threat Intelligence information to keep up to date with TTPs used by threat actors.
- Businesses should use a security solution that provides vulnerability, patch management and exploit prevention components, such as the Automatic Exploit Prevention component in Kaspersky Endpoint Security for Business. The component monitors suspicious actions in applications and blocks malicious file execution.
- Use solutions like Kaspersky Endpoint Detection and Response and Kaspersky Managed Detection and Response service, which help identify and stop an attack at an early stage before the attackers achieve their final goal.

IoC

MD5
ef32824c7388a848c263deb4c360fd64
e58b75e1f588508de7c15a35e2553b86
e89dbc1097cfb8591430ff93d9952260

URL
hidusi[.]com
103.231.14[.]134

MALWARE DESCRIPTIONS | MICROSOFT | MICROSOFT INTERNET EXPLORER | PROOF-OF-CONCEPT | SECURITY TECHNOLOGY | TARGETED ATTACKS | VULNERABILITIES AND EXPLOITS | ZERO-DAY VULNERABILITIES

Authors

AMR

Exploitation of the CVE-2021-40444 vulnerability in MSHTML

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Save my name, email, and website in this browser for the next time I comment.

Notify me when new comments are added.

Comment

// LATEST POSTS

Threat landscape for industrial automation systems in H1 2021

KASPERSKY ICS CERT

Applied YARA training Q&A

COSTIN RAIU, VICENTE DIAZ, VICTOR M. ALVAREZ

QakBot technical analysis

ANTON KUZMENKO, OLEG KUPREEV, HAIM ZIGEL

Triada Trojan in WhatsApp mod

IGOR GOLOVIN

// REPORTS

APT trends report Q2 2021

This is our latest summary of advanced persistent threat (APT) activity, focusing on significant events that we observed during Q2 2021: attacks against Microsoft Exchange servers, APT29 and APT31 activities, targeting campaigns, etc.

LuminousMoth APT: Sweeping attacks for the chosen few

WildPressure targets the macOS platform

Ferocious Kitten: 6 years of covert surveillance in Iran

// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

Email

I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

Threats

Categories

Archive

All tags

Webinars

kaspersky

Privacy Policy | License Agreement