

Remote Code Execution Zero-Day (CVE-2021-40444) Hits Windows, Triggered Via Office Docs

By Trend Micro Sep 09, 2021 Read time: 2 min (453 words)

Published: 2021-09-09 · Archived: 2026-04-05 17:20:58 UTC

Exploits & Vulnerabilities

Microsoft has disclosed the existence of a new zero-day vulnerability that affects multiple versions of Windows. This vulnerability (designated as CVE-2021-40444) is currently delivered via malicious Office 365 documents and requires user input to open the file to trigger.

Microsoft has disclosed the existence of a new zero-day vulnerability that affects multiple versions of Windows. This vulnerability (designated as [CVE-2021-40444open on a new tab](#)) is currently delivered via malicious Office 365 documents and requires user input to open the file to trigger. It should be noted that by default, Office documents downloaded from the internet are opened either in [Protected Viewopen on a new tab](#) or [Application Guardopen on a new tab](#), both of which would mitigate this particular attack.

If the attacker is able to convince the victim to download the file and bypass any mitigation, it would trigger the vulnerability and cause a malicious file to be downloaded and run on the affected machine. Currently, this vulnerability is used to deliver Cobalt Strike payloads.

Microsoft has issued an official bulletin covering this vulnerability. This blog entry discusses how the exploit may work, as well as Trend Micro solutions.

We have obtained multiple samples of documents that exploit this vulnerability. The documents all contain the following code in the *document.xml.rels* file in their package:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId8" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml" />
  <Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml" />
  <Relationship Id="rId7" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml" />
  <Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml" />
  <Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml" />
  <Relationship Id="rId6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target="mhtml:
  /side.html" TargetMode="External" />
  <Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image2.wmf" />
  <Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image1.jpeg" />
</Relationships>
```

Figure 1. Code with XML relationships

Note the presence of a URL (which we have removed) that downloads a file titled *side.html* (SHA-256: d0fd7acc38b3105facd6995344242f28e45f5384c0dfd2ec93ea24bfb1dc9e6). This file contained obfuscated JavaScript; the image in Figure 2 shows part of the deobfuscated code.

We will update this post as necessary if more information becomes available. Updates on Trend Micro solutions can be found on this [knowledge base page](#)[open on a new tab](#).

Indicators of Compromise

SHA-256	File Description	Detection Name
1fb13a158aff3d258b8f62fe211fabeed03f0763b2acadbccad9e8e39969ea00	Payload (CAB)	Trojan.Win64.COBEACON.SUZ
5b85dbe49b8bc1e65e01414a0508329dc41dc13c92c08a4f14c71e3044b06185	Exploited Doc	Trojan.W97M.CVE202140444.A
3bddb2e1a85a9e06b9f9021ad301fdcde33e197225ae1676b8c6d0b416193ecf		
199b9e9a7533431731fbb08ff19d437de1de6533f3ebbf1e13eeffaa4fd455		
938545f7bbe40738908a95da8cdeabb2a11ce2ca36b0f6a74deda9378d380a52		
d0e1f97dbe2d0af9342e64d460527b088d85f96d38b1d1d4aa610c0987dca745		
a5f55361eff96ff070818640d417d2c822f9ae1cdd7e8fa0db943f37f6494db9		
6eedf45cb91f6762de4e35e36bcb03e5ad60ce9ac5a08caeb7eda035cd74762b	Payload (DLL)	Backdoor.Win64.COBEACON.OSI
d0fd7acc38b3105facd6995344242f28e45f5384c0fdf2ec93ea24bfbcb1dc9e6	Downloaded JS	Trojan.JS.TIVEX.A

URL	Category
hxxp://hidusi[.]com/	Malware Accomplice
hxxp://hidusi[.]com/e273caf2ca371919/mountain[.]html	
hxxp://hidusi[.]com/94cc140dcee6068a/help[.]html	
hxxp://hidusi[.]com/e8c76295a5f9acb7/side[.]html	
hxxp://hidusi[.]com/e8c76295a5f9acb7/ministry[.]cab	
hxxps://joxinu[.]com	C&C Server
hxxps://joxinu[.]com/hr[.]html	
hxxps://dodefoh[.]com	
hxxps://dodefoh[.]com/ml[.]html	
hxxp://pawevi[.]com/e32c8df2cf6b7a16/specify.html	
hxxp://sagoge[.]com/	Malware Accomplice
hxxps://comecal[.]com/	
hxxps://rexagi[.]com/	
hxxp://sagoge[.]com/get_load	
hxxps://comecal[.]com/static-directory/templates[.]gif	
hxxps://comecal[.]com/ml[.]js?restart=false	

hxxps://comecal[.]com/avatars
hxxps://rexagi[.]com:443/avatars
hxxps://rexagi[.]com/ml[.]js?restart=false
hxxps://macuwuf[.]com
hxxps://macuwuf[.]com/get_load

Tags

Source: https://www.trendmicro.com/en_us/research/21/i/remote-code-execution-zero-day--cve-2021-40444--hits-windows--tr.html