DotNetNuke CMS 9.5.0 Cross Site Scripting

Authored by Sajjad Pourali

Posted Feb 24, 2020

Cross site scripting attacks can be launched against DotNetNuke CMS version 9.5.0 by uploading a malicious XML file.

tags | exploit, xss
advisories | CVE-2020-5186
SHA-256 | 684ec5f82a14d391aa0415bab3df31b22c06b2ee51e1001641a742fe6b4c2b9e **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-2020-5186
# More Info: https://medium.com/@SajjadPourali/dnn-dotnetnuke-cms-not-as-secure-as-you-think-e8516f789175

DNN allows normal users to upload XML files by using journal tools in their profile. An attacker could upload
XML files which may execute malicious scripts in the user’s browser.

In XML, a namespace is an identifier used to distinguish between XML element names and attribute names which
might be the same. One of the standard namespaces is “http://www.w3.org/1999/xhtml” which permits us to run
XHTML tags such as <script>.

For instance, uploading the following code as an XML file executes javascript and shows a non-harmful ‘XSS’
alert.

<?xml version="1.0" encoding="UTF-8"?>
<script xmlns="http://www.w3.org/1999/xhtml">
alert('XSS');
</script>

Though stealing of authentication cookies are not possible at this time (because the authentication’s cookies
are set as HttpOnly by default), XSS attacks are not limited to stealing users’ cookies. Using XSS
vulnerability, an attacker can perform other more damaging attacks on other or high privileged users, for
example, bypassing CSRF protections which allows uploading “aspx” extension files through settings page which
leads to upload of backdoor files.
```

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