DotNetNuke CMS 9.4.4 Zip Directory Traversal

Authored by Sajjad Pourali

Posted Feb 24, 2020

DotNetNuke CMS version 9.4.4 suffers from zip split issue where a directory traversal attack can be performed to overwrite files or execute malicious code.

tags | exploit, file inclusion
advisories | CVE-2020-5187
SHA-256 | d7f640e068cc427c77cf0775692e1b37581935a6fffb794aa7b0884bad7c39e4 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Zip Slip vulnerability
# Date: 23 Feb 2020
# Exploit Author: Sajjad Pourali
# Vendor Homepage: http://dnnsoftware.com/
# Software Link:
https://github.com/dnnsoftware/Dnn.Platform/releases/download/v9.4.4/DNN_Platform_9.4.4_Install.zip
# Version: <= 9.4.4
# CVE : CVE-2020-5187
# More Info: https://medium.com/@SajjadPourali/dnn-dotnetnuke-cms-not-as-secure-as-you-think-e8516f789175

In a nutshell, Zip Slip is a kind of "directory traversal" attack, which exploits lack of directory names check
while extracting archives. Using this vulnerability attacker may overwrite files with specific extensions on
the system and may execute malicious code.

The zip file extraction function of DNN file upload feature is vulnerable to zip split until 9.5 version (9.5
is not vulnerable).

An attacker could replace any files with following extension on system -

"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"

Ideally, only high privileged user is allowed to upload zip files, but using Vulnerability CVE-2020-5188 –
extension bypass(CVE-2020-5188), a normal user can exploit this vulnerability. For example, a normal privileged
user can replace CSS files on web application and perform defacement of the website.
```

Login or Register to add favorites

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