NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

DOTNETNUKE REMOTE CODE EXECUTION VULNERABILITY CVE®[1]-2017-9822

DISCUSSION

DotNetNuke®[2] (DNN), also known as DNN Evoq and DNN Evoq Engage, is a web-based Content Management System (CMS) developed on the Microsoft®[3] .NET framework. DNN is a web application commonly deployed on local or cloud Microsoft Internet Information Service (IIS) servers.

On July 7, 2017, security researchers revealed a vulnerability within DNN versions 5.2.0 through 9.1.0 that allows an attacker to forge valid DNN credentials and execute arbitrary commands on DNN web servers.

Web-based applications, such as DNN, can be overlooked in routine patching since vulnerability scans may be unaware of their presence. Furthermore, administrators often postpone major version updates to web applications due to the frequent user impact and incompatibility with customized features. Web applications are a frequent target for attackers and vulnerabilities can be exploited days or even hours after their release. For this reason, configuring web applications to update automatically is imperative to secure web application servers.

There are many web-based CMSs similar to DNN. Other common CMS's are WordPress®[4], Drupal®[5] and Joomla®[6]. Organizations should be aware of CMS instances within their purview (i.e., blog, wiki, etc.) and ensure adequate processes are in place for timely updates.

MITIGATION ACTIONS

The most effective mitigation action is to update to the latest version of DNN, version 9.1.1, which is not vulnerable. A hotfix is available at dnnsoftware.com for older versions of DNN, but NSA recommends to only use the hotfix as a temporary measure while migrating to the latest version.

Additionally, the DNN Corporation advocates the use of a scanning tool[7] released by the DNN community that may help to identify sites that have been compromised by an attacker. While this tool may help to identify a compromised site, NSA also recommends using other techniques such as comparing DNN instances against a known good baseline.

APPLICABILITY

This Advisory is issued under the authority defined in National Security Directive 42 and applies to all Executive Departments and Agencies, and to all U.S. Government contractors and agents who operate or use National Security Systems (NSS) as defined in CNSS 4009.

---

[1] CVE is a registered trademark of The MITRE Corporation

[2] DotNetNuke is a registered trademark of the DNN Corporation

[3] Microsoft is a registered trademark of the Microsoft Corporation

[4] WordPress is a registered trademark of the WordPress Foundation

[5] Drupal is a registered trademark of Dries Buyteant

[6] Joomla is a registered trademark of the Open Source Matters, Inc.

[7] https://github.com/DNNCommunity/SecurityAnalyzer/releases

DISCLAIMER OF WARRANTIES AND ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

CONTACT INFORMATION

Client Requirements and General Cybersecurity Inquiries:

Cybersecurity Requirements Center

410-854-4200

Email: Cybersecurity_Requests@nsa.gov