

SECURITY ADVISORY June 2007

DotNetNuke 4.5.3 Phishing Risk in Link Code



Table of Contents

The Security Research Team.....	2
Brief Issue Description.....	3
Affected Components.....	3
Finding Affected Sites with This Issue.....	3
Issue History	3
Example Attack.....	3
Issue Mitigation	3
CVSS Issue Severity Scores.....	3

Copyright and Disclaimer

The information in this advisory is Copyright 2007 FortConsult A/S. It is provided so that our customers and others understand the risk they may be facing by running affected software on their systems.

In case you wish to copy information from this advisory, you must either copy all of it or refer to this document (including our URL).

No guarantee is provided for the accuracy of this information, or damage you may cause your systems in testing.

The Security Research Team

This advisory has been discovered by FortConsult's Security Research Team (team-member: Niel Nielsen), as part of a general investigation into the security of software used in the IT environments of our financial services customers.

FortConsult is a specialist in technical services within the field of IT security. We are vulnerability experts that help business enterprises to protect themselves against the numerous security threats that exist today – both as impartial consultants and with responsibility for specific tasks. Our primary services are security tests and practically-oriented security consultancy.

For more information: www.fortconsult.net.

Brief Issue Description

This advisory describes a vulnerability in the Content Management System “dotNetNuke” (“DNN”), where users could be tricked to submit login information to an untrusted site.

This could give users of a site using DNN the impression of visiting a trusted site, while entering credentials on a non-trusted site.

This issue is affecting registered users as well as users creating a new account on the system.

Affected Components

Version 4.5 has been proven vulnerable to this issue.

Finding Affected Sites with This Issue

The vulnerability described in this advisory can easily be found by “script kiddie”-style hackers, making non-targeted attacks, by searching Google using “Google Hacking” techniques.

Issue History

June 20 2007	FortConsult discovered this issue
June 20 2007	Vendor informed of the issue
June 20 2007	Vendor confirmed the issue, will be fixed in release 4.5.4.
August 2007	Tentative disclosure date

Example Attack

A hacker can fool users to visiting his site, by using your site as the base URL and adding a link to his site like in the following examples:

Example URL for new user registration:

<http://www.dotnetnuke.com/Home/tabid/510/ctl/Register/Default.aspx?returnurl=http://www.evilsite.net>

Example URL for signing in as already registered user:

<http://www.dotnetnuke.com/Home/tabid/510/ctl/Login/Default.aspx?returnurl=http://www.evilsite.net>

Issue Mitigation

Update to latest available version of the application.

CVSS Issue Severity Scores

The issues described in this advisory have received a base score of 7.7. The score is based on the following criteria.

FortConsult has used the online CVSS calculator found at

<http://www.patchadvisor.com/PatchAdvisor/CVSSCalculator.aspx> to calculate these scores.

BASE METRICS: 7.7

Access Vector:	Remote
Access Complexity:	Low
Authentication:	Not Required
Confidentiality Impact:	Partial
Integrity Impact:	Partial
Availability Impact:	None
Impact Bias:	Integrity

FORTCONSULT

Straight talk on IT security