

[VulnWatch] Buffer Overflow in Netware Web Server PERL Handler

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-07/0042.html>

From: Uffe Nielsen (uni_at_protego.dk)

Date: 07/23/03

To: <vulnwatch@vulnwatch.org>, <bugtraq@securityfocus.com>, <news@securiteam.com>

Date: Wed, 23 Jul 2003 16:17:46 +0200

Topic: Buffer Overflow in Netware Web Server PERL Handler

Platform : Netware 5.1 SP6, Netware 6 under certain conditions.

Application : NetWare Enterprise Web Server

Advisory URL: <http://www.protego.dk/advisories/200301.html>

Identifiers: CERT: VU# 185593, CVE: CAN-2003-0562

Vendor Name: Novell, Inc.

Vendor URL: <http://www.novell.com>

Vendor contacted: 10-Feb-2003

Public release: 23-Jul-2003

Problem:

The Netware Enterprise Server does not perform proper bounds check on requests passed to the perl interpreter through the perl virtual directory. This results in a buffer overflow condition, when large requests are sent to the perl interpreter.

Details:

The issue can be triggered by requesting the perl virtual directory followed by a long string.

<http://server/perl/aaaaaa...>[Unspecified number of characters]

The vulnerability occurs in the CGI2PERL.NLM module.

Impact:

A request like the above will overrun the allocated buffer and overwrite EIP, causing the server to ABEND and either suspend the process or restart itself, thereby creating a Denial of Service situation.

Corrective actions:

Novell has made a patch for this issue:

<http://support.novell.com/servlet/tidfinder/2966549>

Disclaimer:

The information within this document may change without notice. Use of

VulnWatch: [VulnWatch] Buffer Overflow in Netware Web Server PERL Handler

this information constitutes acceptance for use in an "AS IS" condition. There are NO warranties with regard to this information. In no event shall PROTEGO be liable for any consequences or damages, including direct, indirect, incidental, consequential, loss of business profits or special damages, arising out of or in connection with the use or spread of this information. Any use of this information lies within the user's responsibility. All registered and unregistered trademarks represented in this document are the sole property of their respective owners.