

[VulnWatch] iDEFENSE Security Advisory 11.04.02b: Denial of Service Vulnerability in Xeneo Web Server

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-11/0009.html>

From: David Endler (dendler@idefense.com)

Date: 11/04/02

From: "David Endler" <dendler@idefense.com>

To: vulnwatch@vulnwatch.org

Date: Mon, 4 Nov 2002 00:46:47 -0500

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

iDEFENSE Security Advisory 11.04.02b:

<http://www.idefense.com/advisory/11.04.02b.txt>

Denial of Service Vulnerability in Xeneo Web Server

November 4, 2002

I. BACKGROUND

Northern Solutions' Xeneo Web Server is a "fast, compact web server that makes it easy to set up and administer a web site on the Windows platform." More information about the application is available at <http://www.northern solutions.com/index.php?view=product>

II. DESCRIPTION

Due to the improper handling of a specially crafted web request, remote attackers may launch a denial of service attack against the PHP version of Xeneo. The condition is triggered when the web server receives a request for '%'. Upon successful exploitation, the web server will crash with a Microsoft Visual C++ runtime error message. The following is an example attack URL:

<http://target.server/%>

III. ANALYSIS

Any remote user with access to the application can launch this attack, thereby denying legitimate users access to the server and the contents and/or additional services provided.

IV. DETECTION

Xeneo 2.1.0.0 (PHP version) and 2.0.759.6 are vulnerable.

V. WORKAROUND

Use a filtering web proxy server to help mitigate against exploitation.

VI. VENDOR FIX

Xeneo 2.1.5 and later should fix the problem. The latest release is version 2.1.6.0, and it can be downloaded at http://www.northern solutions.com/downloads/xeneo_php_setup.exe.

VII. CVE INFORMATION

The Mitre Corp.'s Common Vulnerabilities and Exposures (CVE) Project assigned the identification number CAN-2002-1248 to this issue.

VIII. DISCLOSURE TIMELINE

10/06/2002 Issue disclosed to iDEFENSE
10/31/2002 Author notified
10/31/2002 iDEFENSE clients notified
10/31/2002 Response received from Robert Shanahan
(rshan@northern solutions.com)
11/04/2002 Public disclosure

IX. CREDIT

Tamer Sahin (ts@securityoffice.net) discovered this vulnerability.

Get paid for security research
<http://www.idefense.com/contributor.html>

Subscribe to iDEFENSE Advisories:
send email to listserv@idefense.com, subject line: "subscribe"

About iDEFENSE:

iDEFENSE is a global security intelligence company that proactively monitors sources throughout the world — from technical vulnerabilities and hacker profiling to the global spread of viruses and other malicious code. Our security intelligence services provide decision-makers, frontline security professionals and network administrators with timely access to actionable intelligence and decision support on cyber-related threats. For more information, visit <http://www.idefense.com>.

--dave

David Endler, CISSP
Director, Technical Intelligence
iDEFENSE, Inc.
14151 Newbrook Drive
Suite 100
Chantilly, VA 20151
voice: 703-344-2632
fax: 703-961-1071

dendler@idefense.com
www.idefense.com

-----BEGIN PGP SIGNATURE-----

Version: PGP 7.1.2

Comment: [http://pgp.mit.edu:11371/pks/lookup?op=get&](http://pgp.mit.edu:11371/pks/lookup?op=get&key=0x11371)

iQA/AwUBPcYJR0rdNYRLCswqEQJUywCeM2rbz0jGgJ0i56ucyre/UIkGHq0AoONk
5fG1yOAUGjyZjlvE5QGaOua
=Pnv/

-----END PGP SIGNATURE-----

- **Previous message:** [David Endler: "\[VulnWatch\] iDEFENSE Security Advisory 11.04.02a: Pablo FTP Server DoS Vulnerability"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)