

[Full-Disclosure] ByteHoard Directory Traversal Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-10/1247.html>

From: Sintelli SINTRAQ (sintraq_at_sintelli.com)

Date: 10/19/03

To: <full-disclosure@lists.netsys.com>, <bugtraq@securityfocus.com>

Date: Sun, 19 Oct 2003 20:16:29 +0100

ByteHoard Directory Traversal Vulnerability

17 October 2003

Original Advisory

<http://www.sintelli.com/adv/sa-2003-03-bytehoard.pdf>

Background

ByteHoard is online storage system whereby users can upload and download their files from anywhere with an Internet connection.

More information about the product is available here:

<http://bytehoard.sourceforge.net/index.php?about>

Description

ByteHoard does not properly validate user-supplied input for URL requests. This allows directory traversal characters to be added to URL request and thus allows directory traversal.

An example is:

<http://victim.com/bytehoard/index.php?infolder=../../../../>

Impact

It is possible for an attacker to view all files on the system.

Versions affected

Version 0.7

Solution

Upgrade to version 0.71

Tar version

http://prdownloads.sourceforge.net/bytehoard/bytehoard_point_seven_one.tar.gz?download

Zip version

Full-Disclosure: [Full-Disclosure] ByteHoard Directory Traversal Vulnerability

http://prdownloads.sourceforge.net/bytehoard/bytehoard_point_seven_one.zip?download

Vulnerability History

16 Oct 2003 Identified by Ezhilan of Sintelli
17 Oct 2003 Issue disclosed to ByteHoard developer (Andrew Godwin)
17 Oct 2003 Vulnerability confirmed by Andrew Godwin
17 Oct 2003 Sintelli provided with fix
17 Oct 2003 Sintelli confirms vulnerability has been addressed
17 Oct 2003 Fix publicly available
17 Oct 2003 Sintelli Public Disclosure

Credit

Ezhilan of Sintelli discovered this vulnerability.

About Sintelli:

Sintelli is the world's largest provider of security intelligence solutions. Sintelli is the definitive source for IT Security intelligence and is a provider of third generation intelligence security solutions.

Request a free trial of our alerting solution by clicking here

<http://www.sintelli.com/free-trial.htm>

Copyright 2003 Sintelli Limited. All rights reserved. www.sintelli.com

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>