

# [resend] Strumpf Noir Society on BadBlue

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-01/0242.html>

---

**From:** Strumpf Noir Society ([vuln-dev@labs.secureance.com](mailto:vuln-dev@labs.secureance.com))

**Date:** 01/21/02

Date: Mon, 21 Jan 2002 15:07:15 +0100

From: Strumpf Noir Society <[vuln-dev@labs.secureance.com](mailto:vuln-dev@labs.secureance.com)>

To: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)

Strumpf Noir Society Summaries

! Public release !

<--#

-- Strumpf Noir Society on BadBlue --

(Sorry, couldn't resist.. Ok, so we might not be able to actually drive a Mach truck, but this seems to do the trick, give or take a few millions :)

Release date: Thursday, January 17, 2002

Introduction

BadBlue is the technology behind Working Resources Inc.'s product line with the same name and which, amongst other things, also powers Deerfield.com's D2Gfx file sharing community.

Working Resources Inc. : <http://www.badblue.com>

Deerfield's D2Gfx : <http://d2gfx.deerfield.com>

Summary

Below advisory will serve as a summary for our advisories sns2k2-badblue2 through sns2k-badblue6. These are all more or less related problems in mentioned software and we would not want to annoy too many people at once by sending out five advisories for one product, let's leave some for next time eh?

(More details are available from our web site [1].)

Introduction

The BadBlue technology suffers from multiple vulnerabilities which allow for a resource exhaustion attack to be executed against the server and which could be abused to obtain read access to any file and to

## SecurityFocus Bugtraq: [resend] Strumpf Noir Society on BadBlue

execute system commands on the target host.

When the going goes wrong, part 1:

BadBlue's main purposes are web serving and peer-to-peer file sharing. Due to configuration issues between these functionalities, it is possible to defeat the server's authentication schemes to execute commands on the system. Three different approaches have been found to easily circumvent BadBlue's ip-based authentication. For these attacks to work, the attacker will need to have upload access to either a shared or virtual directory on the target system, or has to trick the system owner into putting his files in such a directory for him.

Of all tested systems only BadBlue EE seems to include this upload functionality and as such is the only system directly vulnerable to these attacks. We feel however that these vulnerabilities represent certain implementation issues in the whole of the product line. These will be looked into by Working Resources Inc. in the next release of their product.

The attacks themselves consist of administrative command execution through PHP or CGI-equivalent scripting, administrative command execution through HTML tags and system command execution through MS Word macros.

Vulnerable:

- BadBlue Enterprise Edition (v1.5.?) for Win9x/NT/2000/ME/XP

Mentioned problems DO work on other versions of the software as well, however it will require some social engineering to get the malicious files in an accessible directory on the server.

When the going goes wrong, part 2:

BadBlue includes the ability to serve transcoded MS Office document data over the web through a number of scripts/templates. More specifically, the server is compatible with MS Word, MS Excel and MS Access. Due to two problems found to be shared in the accompanying scripts doc.htx, xls.htx and mdb.htx however, it is possible to remotely spawn multiple instances of mentioned MS Office applications on the target system. This could be abused in the form of a resource exhaustion attack. Also, there exists a directory traversal attack in the parsers for these documents, which could allow an attacker read access to any file on the target system. All systems tested (BadBlue as well as D2Gfx) were vulnerable to these problems.

Vulnerable:

- BadBlue Personal Edition (v1.5.6 Beta) for Win95/NT4
- BadBlue Personal Edition (v1.5.6 Beta) for Win98/2000/ME/XP
- BadBlue Enterprise Edition (v1.5.?) for Win95/NT4
- BadBlue Enterprise Edition (v1.5.?) for Win98/2000/ME/XP
- Deerfield D2Gfx (v1.0.2 - Effectively BadBlue v1.0.2) for

## SecurityFocus Bugtraq: [resend] Strumpf Noir Society on BadBlue

Win9x/NT/2000/ME/XP

All earlier versions which include mentioned .htx files are expected to be fully or partially vulnerable to these problems.

Vendor status:

Vendor has been notified and has verified above issues. Currently a new version of the BadBlue software is in the making, however no release date for this was available at this time. Since some of the mentioned vulnerabilities leave a users system rather wide open, we've decided to post information on these issues and temporary workarounds. Users are encouraged to upgrade as soon as the new BadBlue release comes available.

Workarounds/fixes:

- 1) Do not allow uploads to directories which can be accessed from the server. This means virtual AS WELL AS shared directories.
- 2) If you have no use for the MS Office document sharing functions of BadBlue, delete/rename/replace the following files: doc.htx, xls.htx and mdb.htx.
- 3) If you do share MS Office documents through BadBlue, share them as single files (meaning: do not select the "Share all files in this folder (\*.\*)" option.
- 4) Limit the number of IP's to which your BadBlue server is accessible to as few as possible through the "Restrict access by IP address" menu under the "Advanced web server functions".

A possible fifth and final recommendation would be to disable IRC sharing. This can be done in BadBlue's "Set your searching options" menu. Although not a security issue perse, this feature is enabled by default in the BadBlue server installation (not in the D2Gfx version btw, which uses an older version of the BadBlue technology) and, besides some information disclosure, makes life quite a lot easier for anyone trying to find potential targets. Alternatives will be included in the next BadBlue release.

References:

Full advisories available from <http://labs.secureance.com>:

sns2k2-badblue2-adv: "BadBlue Scripting Directory Traversal Vulnerability"  
sns2k2-badblue3-adv: "BadBlue Extensions Authentication Bypassing Vulnerability"  
sns2k2-badblue4-adv: "BadBlue Scripting Resource Exhaustion Vulnerability"  
sns2k2-badblue5-adv: "BadBlue HTML Tag Command Execution Vulnerability"  
sns2k2-badblue6-adv: "BadBlue Macro Execution Vulnerability"

yadayadayada

[resend] Strumpf Noir Society on BadBlue

SecurityFocus Bugtraq: [resend] Strumpf Noir Society on BadBlue

SNS Research is rfpolicy (<http://www.wiretrip.net/rfp/policy.html>) compliant, all information is provided on AS IS basis.

EOF, but Strumpf Noir Society will return!

---

- ***Previous message:*** Strumpf Noir Society: "[resend] Avirt Gateway Telnet Vulnerability (and more?)"
- ***Messages sorted by:*** [ date ] [ thread ] [ subject ] [ author ] [ attachment ]