

[NEWS] VICE Emulator Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-06/0033.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/14/04

To: list@securiteam.com

Date: 14 Jun 2004 10:52:01 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

VICE Emulator Format String Vulnerability

SUMMARY

<<http://www.viceteam.org/>> VICE is "a program that runs on a UNIX, MS-DOS, Win32, OS/2, Acorn RISC OS or BeOS machine and executes programs intended for the old 8-bit Commodore computers. The current version emulates the C64, the C128, the VIC20, all the PET models (except the SuperPET 9000, which is out of line anyway), the PLUS4 and the CBM-II (a.k.a. C610)".

There is a format string vulnerability in the handling of the monitor "memory dump" command. If the string to be output contains any % sign, it is interpreted as a command for the output, normally resulting in a crash. Even more sophisticated exploits, like arbitrary code execution on the host machine, are possible.

DETAILS

Vulnerable Systems:

* VICE version 1.6 up to version 1.14 on all platforms

Impact:

It is possible to crash the emulator or even execute arbitrary code on the host machine from the inside of the emulated machine. For this, an

Securiteam: [NEWS] VICE Emulator Format String Vulnerability

attacker needs to fill up parts of the memory with a specific value and wheedle the user to enter the monitor and type in a specific command.

Without the user being wheedled to enter the monitor and type in that specific command, this vulnerability is not exploitable.

Solution:

Upgrade to a newer version of VICE as soon as it becomes available, or use the attached security patch at:

<http://www.trikaliotis.net/vicekb/vice-1.14-mon-vuln.diff.gz>

<http://www.trikaliotis.net/vicekb/vice-1.14-mon-vuln.diff.gz>.

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0453>

CAN-2004-0453

Disclosure Timeline:

June 8, 2004: The VICE team has been informed about this vulnerability

June 8, 2004: The VICE team releases an internal patch the fix this vulnerability

June 10, 2004: First Linux distributors are being contacted.

June 14, 2004: Publication of this flaw

ADDITIONAL INFORMATION

The information has been provided by trik-news@gmx.de Spiro Trikaliotis.

The original article can be found at:

<http://www.trikaliotis.net/vicekb/vsa-2004-1>

<http://www.trikaliotis.net/vicekb/vsa-2004-1>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.