

[UNIX] Exploitable Buffer Overflow in gv

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0104.html>

From: support@securiteam.com

Date: 09/30/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 30 Sep 2002 10:53:20 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Exploitable Buffer Overflow in gv

SUMMARY

The gv program that is shipped on many UNIX systems contains a buffer overflow that can be exploited by an attacker sending a malformed postscript or Adobe PDF file. The attacker would be able to cause arbitrary code to run with the privileges of the victim on his Linux computer. The gv program is a PDF and postscript-viewing program for UNIX that interfaces with the ghostscript interpreter. It is maintained at <http://www.thep.physik.uni-mainz.de/~plass/gv/> by Johannes Plass. This particular security vulnerability occurs in the source code where an unsafe `sscanf()` call is used to interpret PostScript and PDF files.

DETAILS

Analysis:

In order to perform exploitation, an attacker would have to trick a user into viewing a malformed PDF or PostScript file from the command line. This may be somewhat easier for UNIX based email programs that associate gv with email attachments. Since gv is not normally installed setuid root, an attacker would only be able to cause arbitrary code to run with the privileges of that user. Other programs that utilize derivatives of gv, such as `ggv` or `kghostview`, may also be vulnerable in similar ways.

