

[VulnWatch] SunPCi II VNC weak authentication scheme vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-07/0007.html>

From: Richard van den Berg (richard@trust-factory.com)

Date: 07/03/02

Date: Wed, 3 Jul 2002 17:38:42 +0200

From: Richard van den Berg <richard@trust-factory.com>

To: bugtraq@securityfocus.com, vulnwatch@vulnwatch.org, cert@cert.org, submissions@packetstormsec.com

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

Hash: SHA1

Trust Factory Security Advisory TF20020601

Discovery Date: June 2, 2002

Release Date: July 3, 2002

ID: TF20020601

Title: SunPCi II VNC weak authentication scheme vulnerability

Impact: Remote attackers can gain access to the system

Affected Technology: Solaris 2.6, 7, 8 Sparc PCI Platforms using SunPCi 2.3

Sun package: SUNWspvnc version 1.0

Vendor Status: Vendor notified on June 2, 2002

Assigned Sunsolve Bug ID: 4698566

Discovered By: Richard van den Berg <richard@trust-factory.com>

Advisory URL: <http://www.trust-factory.com/TF20020601.html>

Description:

SunPCi II is a PCI daughterboard for Sun Sparc systems capable of running Microsoft Windows OS and applications using an Intel Celeron processor. Starting with version 2.3 of the SunPCi II drivers, Sun ships a modified copy of AT&T's Virtual Network Computing (VNC) client and server. One of the modifications is the authorization process between VNC client and VNC server. The new authentication scheme enables an attacker to discover the VNC password (which is a valid Solaris password) just by sniffing the network between VNC client and VNC server. Once the password is discovered, the attacker can gain access to the system using VNC or other protocols. By default the VNC server is running an X desktop as root.

Technical details:

The readme of the supplied source code of the altered VNC software mentions:

VulnWatch: [VulnWatch] SunPCi II VNC weak authentication scheme vulnerability

-----Start Quote-----

The original authorization code worked as follows:

Server-> password was read/decrypted from file
Server-> sent random bytes to client
Client-> get password from user
Client-> reads random bytes from server
Client-> encrypt random bytes with password
Client-> write encrypted random bytes to server
Server-> reads encrypted random bytes
Server-> encrypts original random bytes using password from file
Server-> compares encrypted random bytes

The new authorization code works as follows:

Server-> sent random bytes to client
Client-> get password from user
Client-> reads random bytes from server
Client-> encrypt password with random bytes as key
Client-> write encrypted password to server
Server-> reads encrypted password
Server-> decrypts encrypted password using random bytes as key
Server-> gets password of current user from system
Server-> encrypts password using user password as salt
Server-> compares encrypted passwords

-----End Quote-----

Since the encryption used by VNC is the well known DES, it is easy to see how this change of code weakens the security significantly. In the original scheme it is difficult to reverse the encryption since the key is an unknown password. (An attacker would need to break into the system first and read it from the file mentioned in the first step.) In the new code, the key used for encryption is the readily available challenge ("random bytes") sent by the server.

Conclusion:

Although encryption is being used, the way it is applied does not add any security to sending the password over the wire in plain text. The original VNC method is much more secure.

Proof of concept:

This requires merely an implementation of the DES algorithm. See attachment.

Work arounds (pick at least one):

- a) Do not use the VNC software supplied by the SUNWspvnc package.
- b) Replace the modified VNC software with the original VNC package
- c) Only use the modified VNC software over a secure channel (i.e. ssh)

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

Version: GnuPG v1.0.6 (GNU/Linux)

Comment: For info see <http://www.gnupg.org>

VulnWatch: [VulnWatch] SunPCi II VNC weak authentication scheme vulnerability

iD8DBQE9IxiiuNOCmWYU0qwRAh/DAKDnCuADHUVsPGDYENAHyU72+wPb4gCg8/uR
KX2XX0Coco2uVERrIwQWNSw=
=4ohf
-----END PGP SIGNATURE-----

--
Richard van den Berg, CISSP

Trust Factory B.V. | <http://www.trust-factory.com/> Bazarstraat 44a | Phone: +31 70 3620684 NL-2518AK
The Hague | Fax : +31 70 3603009 The Netherlands |

- text/x-csrc attachment: [vnCSunpci.c](#)
-

- **Previous message:** [NGSSoftware Insight Security Research: "\[VulnWatch\] Remotely Exploitable Buffer Overruns in Microsoft's Commerce Server 2000/2 \(#NISR03062002\)"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)