

[NT] Security Flaw in Indentix BioLogon Client for Windows

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0041.html>

From: support@securiteam.com

Date: 08/06/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] Security Flaw in Indentix BioLogon Client for Windows

Message-Id: <20010806124509.D046213903@mail.der-keiler.de>

Date: Mon, 6 Aug 2001 14:45:09 +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>

Security Flaw in Indentix BioLogon Client for Windows

SUMMARY

<<http://www.identix.com>> Identix's BioLogon software is used as "glue" to tie together various biometric devices to the Windows operating system. The BioLogon client works with smart cards, fingerprint readers, and other devices that interact with Windows.

A security vulnerability in the product allows attackers to bypass the identification protection used by the program whenever this product is installed on a "multi-monitor" (multi screen) system.

DETAILS

Vulnerable systems:

BioLogon Client version 2.0

The security vulnerability exists when the software is installed onto a Windows system that has more than one video card installed and the system is doing "multi-monitor" with the built in virtual desktop software that comes with Windows 98 SE and Windows 2000.

The problem is that the BioLogon client software attempts to harden the screensaver password locking mechanism so that a biometric device is needed to unlock the system. Unfortunately, the software only locks the first screen (screen zero). No access is blocked from any other screen (virtual desktop). Mouse, keyboard, and the screen can be used while

Hypermail Development List: [NT] Security Flaw in Indentix BioL

screen zero is locked. In fact, unless the mouse is on screen zero, the biometric device will not recognize the fact it should inquire for input.

Vendor response:

Vendor has been contacted, their response was:

"Problem was noted and replicated but that it is a very low priority".

ADDITIONAL INFORMATION

The information has been provided by <mailto:Marc.DeBonis@VT.EDU> Marc DeBonis.

=====

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.

-
- *Next message:* support@securiteam.com: "[TOOL] SnortSperm, a DCShop Order and Account Scanner"
 - *Previous message:* support@securiteam.com: "[EXPL] ARPNuke, Windows Network Nuker"
 - *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)