Lucent Technologies, Inc. VitalSuite Security Bulletin

Bulletin Number: #00201
Date: January 21, 2002
Cross-Ref: Patch 2732
Title: VS URL, No Passwords

---

1. Bulletin Topics

Lucent announces the release of patches for Vitalsuite 8.0, 8.1 and 8.2 products including VitalNet, VitalHelp/VitalAnalysis, and VitalEvent if separately licensed, or installed together as VitalSuite.
Lucent recommends that you install the patch listed in section 4 immediately on systems running VitalSuite releases 8.0, 8.1 or 8.2.

2. Who is affected

Vulnerable: Lucent VitalSuite, VitalNet, VitalEvent, or VitalHelp/VitalAnalysis releases 8.0, 8.1 or 8.2.

3. Understanding the Vulnerability
A vulnerability has been discovered in VitalSuite that may allow unauthorized users to bypass authentication.

Cookie-based authentication is a feature that was introduced into VitalNet 8.0. However, the implementation of the cookie-based authentication mechanism allows an unauthorized user who guesses a correct username to receive a valid cookie for that user. This will allow the unauthorized user to authenticate to the server without need of a password, using a URL such as the following.

http://<serverip>/cgi-bin/VsSetCookie.exe?vsuser=<account-name>

This allows the unauthorized user to gain access to the VitalSuite server, with privileges assigned to the user account that has been guessed.

This issue was reported by Security Focus who published an advisory:
http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=exploit&id=3784

A DefenseOne Command Center Advisory is also available (for its subscribers) at:

https://www.defenseone-commandcenter.com/vulns/5/3784

A second vulnerability was reported. If a user logs into the VitalSuite server and his account name is the same as his password, no subsequent entry of the password is required to access the server.

4. Available Patches

A patch is available which will prevent the use of such a URL to attempt access to a VitalSuite server. It will also ensure that both

account name and password have been correctly entered prior to allowing account access. Vitalsuite customers are reminded to carefully choose, change and use passwords; maintain Vitalsuite servers behind firewalls where access can be controlled, and to change or delete default account names or passwords.
The following patches are available in relation to the above issue.

Patch 2732

APPENDICES

A. Patch information listed in this bulletin is available to all supported Lucent VitalSuite customers via email:

crc@lucent.com at 888 467-8324

B. Tob obtain a copy of this security bulletin, contact:
Richard Hafner at rhafner@lcuent.com
or Dave Ushler -- dushler@lucent.com (610) 722-7948

C. To report or inquire about a security problem with Lucent VitalSuite software, contact one or more of the following:

- Your local Lucent support engineer
- Your local Lucent account executive
- Lucent Customer Response Center email: CRC@lucent.com

The information contained in this Security Bulletin is provided "AS IS." Lucent makes no warranties of any kind with respect to the information contained in this Security Bulletin. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY WARRANTY OF NON-INFRINGEMENT OR IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE HEREBY DISCLAIMED AND EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

IN NO EVENT WILL LUCENT BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF ANY THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE INFORMATION CONTAINED IN THIS SECURITY BULLETIN, EVEN IF LUCENT TECHNOLOGIES, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

If any of the above provisions are held to be in violation of applicable law, void, or unenforceable in any jurisdiction, then such provisions are waived to the extent necessary for this disclaimer to be otherwise enforceable in such jurisdiction.