


[Subscribe for free](#)
[Browse archive](#)

HELP NET SECURITY

 Search Help Net Security


NEWS

MALWARE

ARTICLES

REVIEWS

Q&As

EVENTS

SOFTWARE

NEWSLETTER

Patch management



GFI LanGuard™
Network security scanner
and patch management

Featured news

- Flaws in medical data management system can be exploited to modify patient information
- How Europol analyzes malware
- The privacy risks of school technology tools
- Belkin's N150 router sports multiple flaws, including default access credentials for telnet server
- Top 10 technology challenges for IT audit professionals
- Lack of visibility and security concerns hinder cloud adoption
- Securing the smart home environment
- Revealed: What info the FBI can collect with a National Security Letter
- VTech data breach gets worse: Children's pictures and chat logs were also compromised
- Windows machines stop trusting Dell's two unconstrained root CA certs
- Why we need digital security forensic analysis
- Hacktivists and cyber extortionists hit Greek, Russian, UAE banks
- Human element of security to the fore at IRISCON 2015
- VPN protocol flaw allows attackers to discover users' true IP address
- Telegram Android app is a stalker's dream
- 900+ embedded devices share hard-coded certs, SSH host keys
- 4 ways an attacker can infiltrate an organization by diverting security solutions

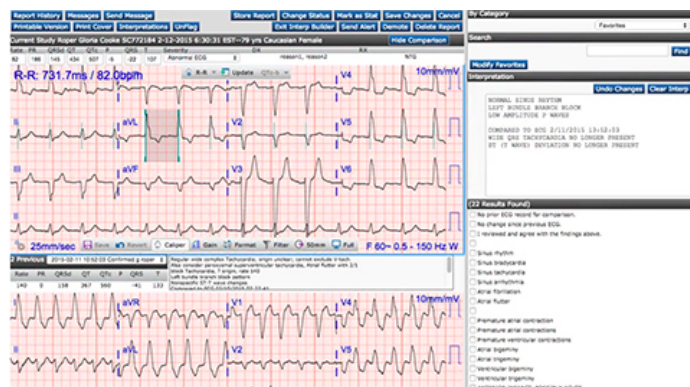
Reduce the risk of data leaks and other malicious activity.

[Download the free trial now!](#)

Flaws in medical data management system can be exploited to modify patient information

Posted on 02 December 2015.

Two vulnerabilities found in v3.3 of Epiphany's Cardio Server ECG Management System, a popular system that is used to centralize and manage patient data by healthcare organizations around the world (but mostly in the US), can be exploited by local attackers to access and modify patient information, [warns](#) CERT/CC.



The system can receive data from a great variety of medical devices, and is usually run on local servers belonging to the organization. It allows users (physicians and other medical personnel) to access all kinds of patient data, including diagnostic test results from anywhere in the hospital, their offices or their homes.

The system is accessible via web browser. The two vulnerabilities, found by Alex Lauerman of infosec consultancy TrustFoundry, affect the system's login page.

An improper neutralization of special elements allows either a SQL command to be inserted into the login page URL, or a LDAP query to be inserted into it. The first issue can lead to an unauthenticated user to get logged in as an administrator, and have access to all the information on the system, and the second one can cause the Cardio Server to perform an LDAP query to the IP address of the attacker's choice.

The issues are present in v3.3 of the system, and possibly in later versions as well. CERT/CC has tried to get in touch with the vendor - Epiphany Healthcare - to check whether later versions (4.x and 5.x) are also affected, but hasn't had much luck.

As Cardio Server version 3.x is end-of-life and no longer receives security updates, the only thing organizations can do is to upgrade to version 4.x or 5.x as soon as possible and to pester the vendor about a fix (if the issues haven't been fixed already).

Author: Zeljka Zorz, HNS Managing Editor

[Follow @zeljkazorz](#)

[exploit](#)
[Internet of Things](#)
[privacy](#)
[software](#)
[vulnerability](#)

Spotlight

1 2 3 4 5

Hacktivists and cyber extortionists hit Greek, Russian, UAE banks

A number of "regular" and central banks across Europe, Russia and Asia have been targeted by cyber attackers. The banks haven't paid the asked-for money and they have managed to put a stop to the attacks, at least for now.

Keep your business secure and compliant

Automatic patch management and vulnerability scanning

GFI LanGuard™
Network security scanner and patch management

Weekly newsletter

Reading our newsletter every Monday will keep you up-to-date with security news.

 Email @ Address

[Subscribe](#)


Daily digest

Receive a daily digest of the latest security news.

 Email @ Address

[Subscribe](#)

Subscribe to the HNS newsletter and win one of these books.
If you win, we'll e-mail you on January 6.



Email Address

Subscribe

DON'T MISS

Wed, Dec 2nd

Flaws in medical data management system can be exploited

The privacy risks of school technology tools

Belkin's N150 router sports multiple flaws

Revealed: What info the FBI can collect with a National Security Letter

VTech data breach gets worse: Children's pictures and chat logs were also compromised

[Back to TOP](#)



Subscribe for free

Browse archive

HELP NET SECURITY

Search Help Net Security



(IN)SECURE

FREE INFOSEC MAGAZINE

COPYRIGHT 1998-2015 BY HELP NET SECURITY. // [READ OUR PRIVACY POLICY](#) // [ABOUT US](#) // [ADVERTISE](#) //