Northwest Shelbyville Regional Hospital

Memo

To: Chris Bailey, Chief Information Security Officer

From: Micah L. Martinez

Date: 02 February 2021

Re: Vulnerabilities Found During IT Audit

After the recent audit of the medical systems and IT infrastructure some vulnerabilities have been found. Below I have listed the devices affected, background on the vulnerabilities, and recommended actions to fix the vulnerabilities.

Device 1: GE Xeleris versions 1.0,1.1,2.1,3.0,3.1

- The GE Xeleris is part of a range of molecular imaging tools designed to enable earlier treatment for patients. The Xeleris workstation allows for automation, personalization, and other advanced applications for use with patient images. However, remote attacks can exploit the default or hard-coded credentials to gain access to patient information. The impact of this vulnerability is Low and varies depending on operational environment and specific usage.
- **CVE ID**: CVE-2017-14006, default/hard-coded credentials can be exploited [1] [2].
- Possible solutions include closing unused ports on the system, changing passwords, discontinue the use of non-product related applications, restrict access, and make sure the most recent software patches are installed.
- I recommend getting help with changing the passwords by contacting GE service, closing any unused ports, and restricting access to only those that need to use these systems.

Device 2: OpenClinic

- OpenClinic is an open-source, medical records viewing system. It is used to manage and edit patient's records, including social data and clinic history. There have been four vulnerabilities found in this software that allow attackers to view and store files, gain remote access, or escalate unauthorized user's access. The impact of this vulnerability is High.
- **CVE ID**: CVE-2020-28937, vulnerabilities allow unauthorized access to PHI, possible escalation of privileges to unauthorized users, or remote access [3] [4].
- At this moment, no version of OpenClinic is immune to these vulnerabilities.
- I recommend ceasing the use of this software and using an alternative medical record management system.

If you have any questions or concerns, please contact me and I will get back to you as soon as possible.

References

[1] The MITRE Corporation, "CVE-2017-14006," 2021. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14006. [Accessed 2 February 2021].

[2] Cybersecurity and Infrascructure Security Agency, "ICS Advisory (ICSMA-18-037-02)," 13 March 2018. [Online]. Available: https://us-cert.cisa.gov/ics/advisories/ICSMA-18-037-02. [Accessed 2 February 2021].

[3] The MITRE Corporation, "CVE-2020-28937," 2021. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28937. [Accessed 2 February 2021].

[4] G. Kleijn, "OpenClinic 0.8.2," 1 December 2020. [Online]. Available: https://labs.bishopfox.com/advisories/openclinic-version-0.8.2. [Accessed 2 February 2021].