nccgroup

Royalty-free stock vector ID: 1108368677

Dec 07, 2020 14:21 GMT

Assessing the cyber risks of connectivity in the healthcare sector

Our lives are more connected than ever – access to services and data is ubiquitous. IoT has had a large part to play in this as IoT devices are everywhere – in our homes, workplaces, dotted across our smart cities and towns.

The healthcare sector is no exception – access to patient services, GP practices and even your patient records, connectivity is becoming more widespread as people take a more proactive role in their wellbeing.

However, it's important to consider the risks this connectivity and its underlying infrastructure brings, especially as sectors like healthcare increase their adoption of connected medical devices.

Providing a holistic view of connectivity in healthcare

Earlier this year, we partnered with The AbedGraham Group – a global healthcare IT and cyber security technology group, made up of physicians and security analysts.

A unique mix of clinical and technical expertise, our partnership with The AbedGraham Group gave us a great opportunity to provide a holistic view of the expanding connected healthcare space. For this, we decided to conduct a risk analysis of the F5 BIG-IP vulnerability and apply this to the healthcare system.

The F5 BIG-IP vulnerability

This vulnerability, which was disclosed in July by Positive Technologies, allows unauthenticated users to read and write files, execute commands and disable services through the BIG IP Traffic Management User Interface (TMUI).

This means that if the TMUI is exposed to the Internet, anyone that can access it would be able to take complete control of the device with full administrative privileges. And depending on the role the device plays and what it is connected to, it could facilitate further attacks and act as a backdoor into an internal network.

F5 BIG-IP vulnerability in a clinical and non-clinical scenario

Working with the AbedGraham Group, we carried out a qualitative and quantitative analysis to showcase the cyber security risks that can be associated with network infrastructure in healthcare within non-clinical and clinical scenarios.

The two scenarios we looked at were:

- *What would be the risk associated with this highly critical vulnerability being present on a F5 BIG-IP Load Balancer, which supports the handling and direction of inbound web traffic from its external facing websites for a healthcare system?*
- *What would be the risk associated with this highly critical vulnerability present on a F5 BIG-IP Load Balancer which supports domain authentication and bandwidth management through the authentication server providing access to the Electronic Health Record (EHR) clinical application within a healthcare system?*

From our analysis, we were able to map out the potential impact of the F5 BIG-IP vulnerability across both scenarios in the healthcare sector, and confirm risks associated to both the medical devices and the network infrastructure that supports these.

This included a disruption to the administrative workflows and communication in the first scenario, which could delay patients making it into the hospital setting and receiving timely care. In the second scenario, the vulnerability would impact a wider range of activities across inpatient, outpatient and community related settings.

Given the function that these devices have, and the network infrastructure that supports mission-critical clinical applications and systems, it's never been more crucial to understand the technical risks.

Commenting on this research, Dr Saif Abed, director of cyber security advisory services at The AbedGraham Group said: "Now more than ever, leaders across healthcare organisations from the CISO to the Chief Medical Officer and CEO need to be able to understand cyber security in terms of patient safety and clinical service disruption. Our research demonstrates that network infrastructure can have a profound impact in both those areas perhaps even more so than vulnerabilities in actual medical devices in many instances.

"By working with NCC Group, we were able to explore these risks from a holistic perspective and quantify their potential impact in a way that can help streamline remediation activities where they matter most."

Stuart Kurutac, senior security consultant at NCC Group added: "As healthcare settings become more connected, the need for enhanced security becomes even greater, especially when a patient's health and life could be at risk.

“While traditional concerns have focused very much on the connected devices, our research with The AbedGraham Group has highlighted that we should never overlook the security risks associated with network infrastructure.”

To find out more about the research and results, download the whitepaper here.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company’s knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970