Security: Summer interns see vulnerabilities in visitor management systems

March 5 2019, by Nancy Cohen

Credit: CC0 Public Domain

For business managers, the goal may be to find a technology-driven process that can protect the security and safety of the premises, staff and visitors. Visitor management systems may not only perform check-ins

but also control access to restricted areas.

"The friendly receptionist or security guard is being replaced by kiosks, and it is big business, with sales expected to exceed $1.3 billion by 2025,"said Daniel Crowley, who heads research for IBM X-Force Red. X-Force Red? Are these tough guys? In a sense, yes. This is a team of hackers in IBM Security. They do attempt break-ins. Their work is to discover vulnerabilities that criminal attackers may use.

So, if businesses may be interested in looking for visitor check in systems, then they had best find something that is more than just a digital log book. Are they finding what they need and is their choice secure? X-Force Red has smelled something wrong. Attackers can steal your data. Attackers can impersonate you.

Sign-in kiosks (portals at businesses and facilities) might be vulnerable to data spying. *Threatpost* was not gentle in its choice of headline: "Visitor Kiosk Access Systems Riddled with Bugs."

Two of the X-Force Red summer interns found 19 previously undisclosed vulnerabilities across five popular visitor management systems.

Threatpost carried some interesting information about what the testing goals were when the team set out to test the visitor-management systems.

"One, was how easy is to get checked-in as a visitor without any sort of real identifying information. Secondly, we set out to see how easy is it to get other people's information out of the system. And third, is there a way that an adversary can break out of the application, cause it to crash or get arbitrary code-execution to run on the targeted device and gain a foothold to attack the corporate network."

Crowley reported on findings in *SecurityIntelligence*: Information disclosure of personal and corporate data; several applications had default administrative credentials; vulnerabilities allowing an attacker to use Windows hotkeys and standard help or print dialogs to break out of the kiosk environment and interact with Windows, such that an attacker would have control over the system with the same privileges as the software was given.

Are some check-in systems incidents waiting to happen? Lily Hay Newman in *Wired* on Monday raised some scenarios that seemed uncomplicated if a person wished to do malice. She said that "a hacker could easily approach a visitor management system with a tool like a USB stick set up to automatically exfiltrate data or install remote-access malware."

In addition, "while faster is always better for an attack," she wrote, "it would be relatively easy to stand at a sign-in kiosk for a few minutes without attracting any suspicion."

Wired said on Monday that the flaws the two found were mostly patched.

"This was sort of scratch-the-surface kind of stuff," Crowley said in *Wired.* If the bugs were seen in just a few weeks, he added, it said "a lot about what else might be lurking on these crucial and interconnected systems. "

What's next: The X-Force Red team provided vulnerability details to affected vendors "in advance in order to allow time for an official fix to be developed and released in advance of this publication," Crowley said. "Several of the vendors have updated their software or plan to with appropriate patches of changes to functions."

TechNadu said some companies claimed user data was never in danger.

Crowley's article in *SecurityIntelligence* also addressed advice.

The advice included: Encrypt everything. "Full-disk encryption should always be used on any system accessible to the public." He said that full-disk encryption was already the norm on iOS devices. Also, he said if network access is not required for the visitor management system to function, it should not be connected to the network.

More information: Stranger Danger: X-Force Red Finds 19 Vulnerabilities in Visitor Management Systems: securityintelligence.com/stran … -management-systems/

Citation: Security: Summer interns see vulnerabilities in visitor management systems (2019, March 5) retrieved 20 April 2024 from https://techxplore.com/news/2019-03-summer-interns-vulnerabilities-visitor.html