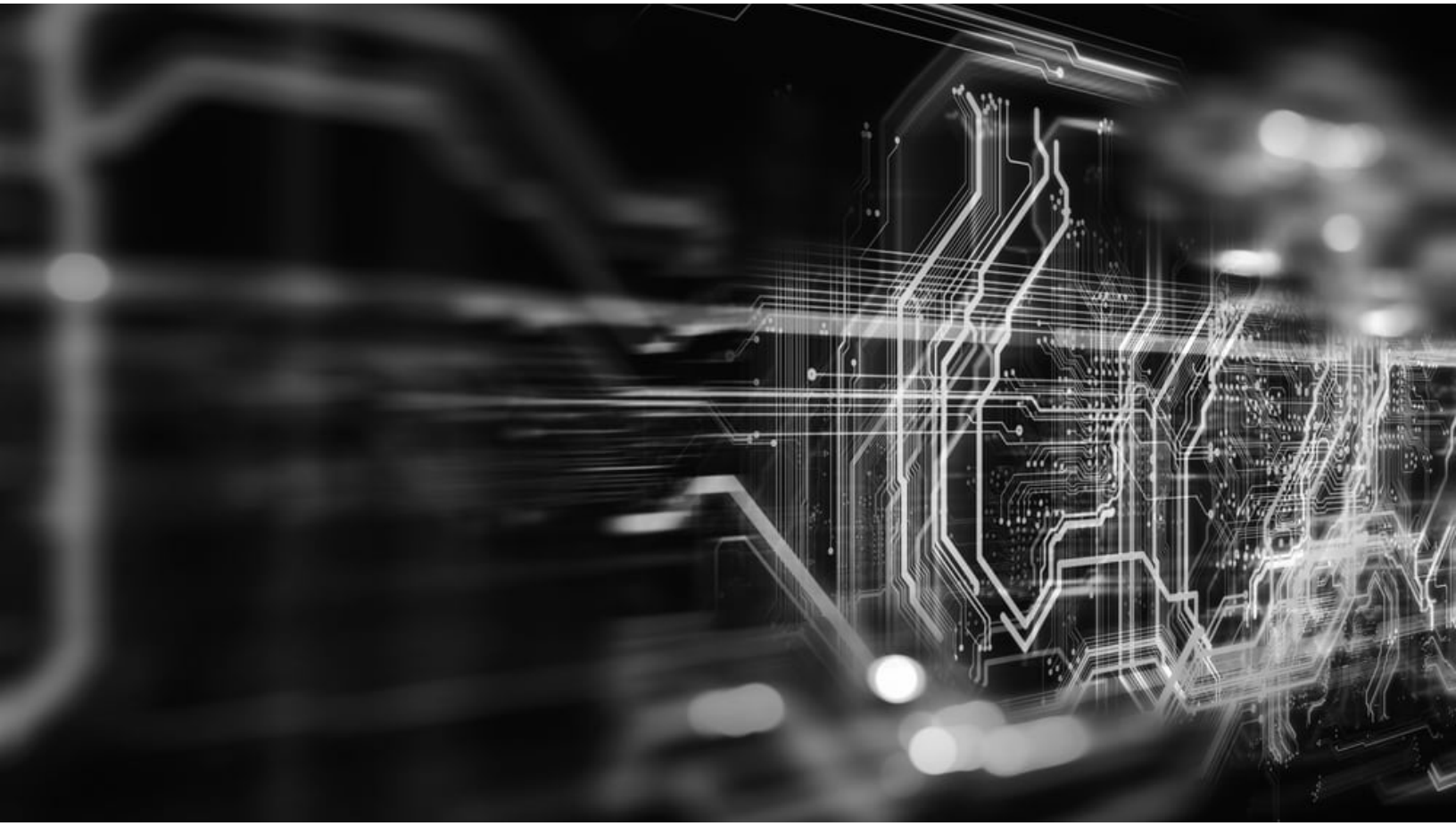
nccgroup



Aug 08, 2019 22:24 BST

The cyber risk lurking in your office corner

The humble office printer has morphed over the years into a full-blown multifunction device capable of a huge range of activities. Today, many enterprise printers can print, scan, copy, fax and email, all within a footprint that's similar to, or smaller than, conventional office printers.

As with all enterprise technology, printers are an essential ingredient to the smooth operation of a business, no matter the size. And while cyber security for much of the enterprise technology in use today has largely advanced over the years in line with the evolving threat landscape, the same can't always be said for enterprise printers. Indeed, security controls for network devices such

as printers are often overlooked.

This is a problem, given that enterprise printers are often used to manage, print or process sensitive information in one way or another. They may seem mundane, but they are connected to just about every device in some organisations, representing a crucial part of the enterprise network that should be secured as much as PCs, shared servers and data storage devices.

This is one of the reasons why NCC Group researchers decided to embark on a six-month project aimed at identifying vulnerabilities and exploitations relating to devices made by six of the largest enterprise printer makers in the world.

Our researchers, Mario Rivas and Daniel Romero, discovered remote vulnerabilities in all of the printers they tested through various attack vectors, uncovering a large number of zero-day vulnerabilities in the process.

The researchers found, among other things, that one of the printers was affected by multiple overflow vulnerabilities in the Internet Printing Protocol (IPP) service, allowing a potential attacker to effect a Denial of Service (DoS) attack and perhaps even execute arbitrary code on the device.

The research undertaken also revealed that some of the printers contained a DoS vulnerability in their Simple Network Management Protocol (SNMP) service. If exploited, this vulnerability could potentially cause the machine to crash.

The good news is that thanks to this research, the manufacturers in question were able to provide updates to close up the identified vulnerabilities and secure the affected devices against the exploits uncovered by the researchers.

However, these examples demonstrate just how careful manufacturers and the enterprises using their devices need to be when it comes to ensuring network-connected printers are up to scratch in terms of cyber security.

This research also demonstrates how important company-wide cyber security strategies involving comprehensive prevention and response measures, such as active monitoring by a security operations centre (SOC), training and

education, penetration testing and security information and event management (SIEM), can be.

While we have already discovered a host of previously unknown vulnerabilities in the humble office printer, there is much more work to be done – by security researchers, enterprise printer manufacturers and the end users of these devices.

Certainly, there's more to the story. And we'll get to hear more of it when Mario and Daniel reveal the full extent of their research at several industry conferences, including DEF CON, Hack In The Box Security Conference and 44CON.

Daniel and Mario will walk attendees through their entire printer research engagement, from threat modelling to the development of attack methodologies and beyond, demonstrating how to use enterprise printers as a method of persistence on a network.

Most importantly, the researchers will present mitigations that printer manufacturers are able to implement if they want to reduce device attack surfaces and make potential exploits more difficult to carry out successfully.

Thanks to researchers like Mario and Daniel, that seemingly innocent printer in the corner of your office is now a little bit safer.

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 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant

market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan 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

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750