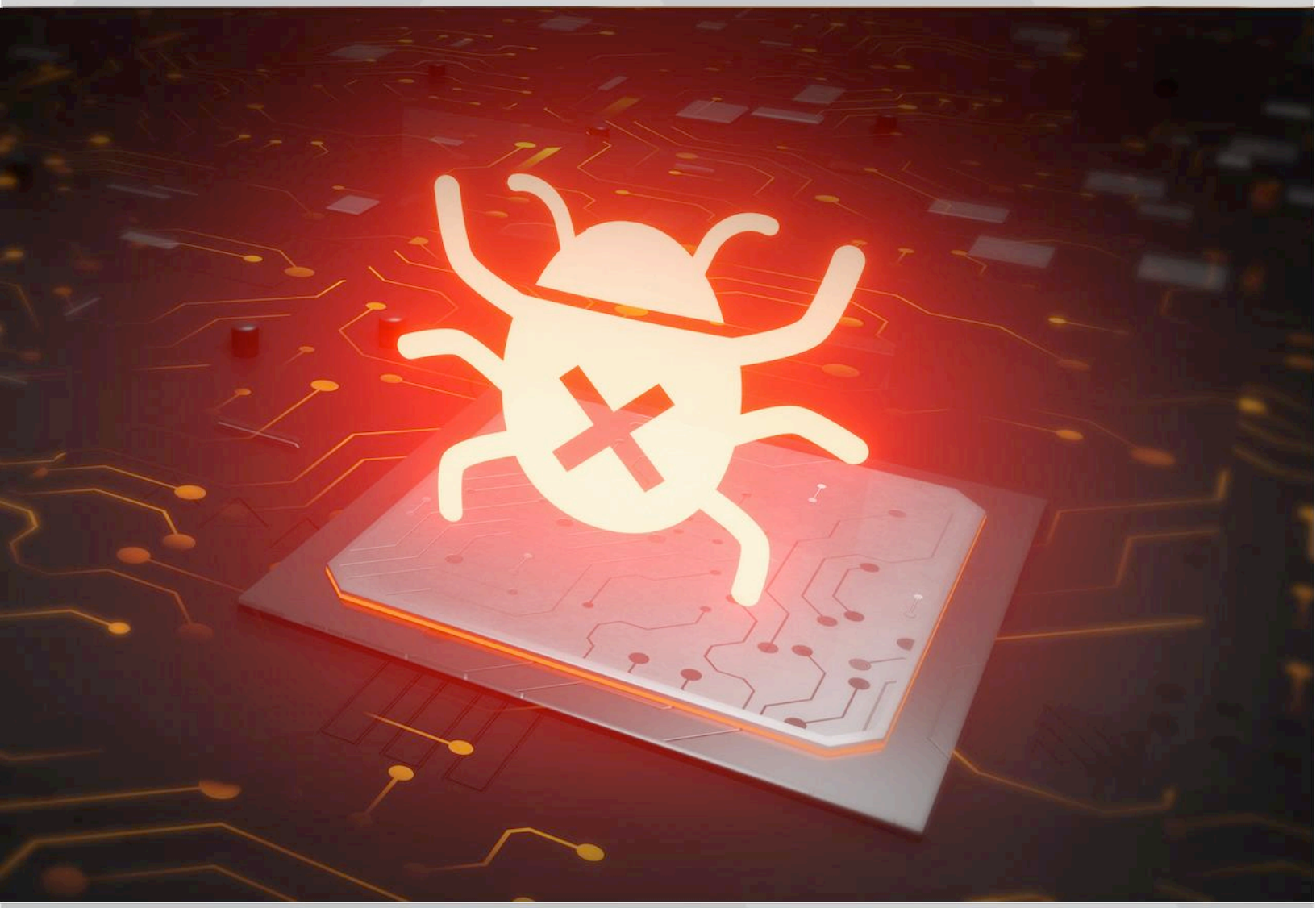
ACTIONABLE INTELLIGENCE

HP Bug Bounty Program Finds Reprogrammable Chips Open Printers to Malware



THE PRINTER AND SUPPLIES INDUSTRY'S LEADER FOR NEWS AND ANALYSIS

HP has confirmed third-party cartridges with reprogrammable chips can be used to inject malware into printers and compromise networks.

HP Inc. reported to Actionable Intelligence that it has confirmed third-party cartridges with reprogrammable chips can be used to inject malware into printers and compromise networks. HP has released a security alert and updated printer firmware to address the problem.

The news, which was shared exclusively with this website, confirms suspicions that HP executives have voiced in the past (see "HP Warns That Third-Party Chips Pose Security Risks"). In recent years, HP representatives have expressed concerns that the reprogrammable chips being released by certain chipmakers for use on non-HP cartridges would make it possible for hackers to reprogram chips with malware and compromise printers. Reasoning the OEM was just spreading FUD (fear, uncertainty, and doubt), the third-party supplies industry reacted with a good deal of skepticism after HP told Actionable Intelligence in 2020 that the key reason for expanding the Bug Bounty program to include cartridges was to explore the possible security risks third-party cartridges featuring non-HP chips might present. Now, the Bug Bounty program has found that the unsettling scenario is indeed possible: Hackers can use reprogrammable cartridge chips to gain a backdoor through printers to larger IT networks.

Shivaun Albright, chief technologist of print security for HP, talked to us about why HP believed reprogrammable third-party cartridges posed a risk back in 2020. Last week, Ms. Albright was joined by Dave Turner, vice president and general manager of toner supplies and solutions for HP, and Steve Daniels, printing supplies security lead for HP, who shared with Actionable Intelligence an update on Bug Bounty. The focus was on what Bug Bounty researchers were able to do with a third-party cartridge featuring a reprogrammable third-party chip.

HP Print Security, Bug Bounty, and Differences between Chips

Before we dive into what hackers were able to do with a third-party cartridge, a little background is in order on HP's focus on security, the Bug Bounty program, and cartridge chips.

Mr. Turner said that HP looks at security as a system, adding that system is "only as strong as its weakest link." The focus, he said, has to be on examining the "printer, the cartridge, and even the supply chain and manufacturing processes." Mr. Turner said, "We look at every component to make sure that they are secure. And our philosophy is that we have to make it better and better. Bug Bounty is a way for us to continuously test the level of defense, the level of security, and our ability to protect against ever evolving, sophisticated attacks."

Ms. Albright declared that print security is part of HP's broader mission of engineering "the world's most secure and resilient devices, technologies, and

© 2023 Actionable Intelligence

HP contracts Bugcrowd's trusted hackers to try to expose weaknesses in its security so HP can fix security flaws before they become a problem for customers.

services." She said, "Over the past 20 years, we have dedicated ourselves to raising the bar in endpoint security with industry defining standards and several 'industry firsts'—from inventing and standardizing modern trusted computing; to designing resilient, self-healing hardware; and leading in IoT and printer security innovation."

Ms. Albright emphasized Bug Bounty is just one element in HP's layered, end-to-end security strategy for printing products. Ms. Albright described HP's print security as a "journey of innovation," noting that the company has been first to market with many key security features. She shared a slide highlighting some of HP's key printing innovations since 2013. In the nearly 10 years since then, HP has continuously rolled out security enhancements and worked to grow customer awareness of how important print security is.

Bug Bounty is part of HP's efforts to harden its printing ecosystem security. When HP releases a new platform or solution, the OEM does its own penetration testing and works with third parties to perform penetration testing.

Starting in 2018, HP added to its penetration testing by rolling out its Bug Bounty program (see "HP's Bug Bounty Program Invites Hackers to Find Printer Security Flaws"). Under this program, HP works with Bugcrowd, a crowd-sourced cyber security organization. HP contracts Bugcrowd's trusted hackers to try to expose weaknesses in its security so HP can fix security flaws before they become a problem for customers. As noted above, the Bug Bounty program was expanded to include security testing of cartridges in 2020.

Ms. Albright explained, "Typical printer attacks can exploit older versions of firmware and allow the device to be taken over and halted operationally. HP is combatting this risk with a layered defense-in-depth approach. We also continue to invest in research and innovation to continuously improve the security of our printing systems." But, Ms. Albright added, "Print security extends beyond the hardware. Office-class print cartridges contain microcontroller chips that communicate with the printer over an electronic data interface. Microcontroller chips on cartridges offer significant

© 2023 Actionable Intelligence

The bottom line, according to Ms. Albright, is that HP's chips are secure and the reprogrammable chips sold by certain chipmakers for use on third-party compatible and remanufactured cartridges are not.

A Bugcrowd researcher working on the Bug Bounty program explored whether it would be possible to break into a printer using a third-party inkjet cartridge with a reprogrammable chip and was able to do exactly that.

customer benefits when it comes to supply management, authentication, and compatibility, but they can also be an ingress point for attacks."

The bottom line, according to Ms. Albright, is that HP's chips are secure and the reprogrammable chips sold by certain chipmakers for use on third-party compatible and remanufactured cartridges are not. According to Ms. Albright, HP uses security-hardened, tamper-resistant chips on its cartridges. HP's chips for office-class devices use secure smartcard technology, commonly found on chip-based credit and debit cards. Moreover, HP works to ensure supply-chain security so chips aren't compromised along their journey into customers' hands.

In fact, HP earned certification demonstrating the security of its supply chain. In 2021, HP enterprise printers and original consumables earned ISO 20243 certification (see "HP Focuses on Work-from-Home Services and Security"). This supply-chain certification validates that HP delivers secure and tamper-resistant printers and supplies and validates that product security and integrity is maintained at each part of the product lifecycle, including design, sourcing, testing, manufacturing, and distribution.

In contrast, Ms. Albright said that third-party chipmakers are selling chips that are reprogrammable, meaning the code can be modified via a resetting tool right in the field. Actionable Intelligence's understanding is that third-party chipmakers have designed chips to be reprogrammable not for nefarious purposes but instead to update chips so that they will still work after an OEM firmware update. Regardless of the intent, HP's view is that because these chips are reprogrammable, they are less secure. The risks are compounded because third-party cartridges and the chips thereon may have a more circuitous, less secure path to customers. The wide availability of technologies that can be used to rewrite third-party chips means there are a lot of different points in any given supply chain where hackers can gain access to a non-HP cartridge and insert malicious code.

Ms. Albright said a potential scenario might involve a hacker who wants to perform targeted espionage at a particular company. She said a hacker could inject malware onto third-party cartridges with rewritable chips and send them out for free, pretending that the cartridges are being sent as a promotion. If those cartridges are installed by an IT department or office manager excited to take advantage of the free cartridges, this is essentially like putting a USB stick infected with malware into your PC. The infected cartridge chip can infect printers and from there gain access to sensitive information and corporate networks.

What Bug Bounty Found

HP is no longer talking about this security risk in the conditional and saying this is something that "could happen." A Bugcrowd researcher working on the Bug Bounty program explored whether it would be possible to break into a printer using a third-party inkjet cartridge with a reprogrammable chip and was able to do exactly that.

Ms. Albright said, "A researcher found a vulnerability over the serial interface between the cartridge and the printer. Essentially, they found a buffer overflow. That's where you have got an interface that you may not have tested or validated well enough, and the hacker was able to overflow into memory beyond the bounds of that particular buffer. And that gives them the ability to inject code into the device."

© 2023 Actionable Intelligence

When the third-party cartridge with the infected chip was installed, the researcher was able to inject malware into the printer using that buffer overflow.

Once the Bug Bounty researcher shared with HP how he was able to take control of a printer using malware on a third-party chip, HP sprang into action.

What the researcher was able to do to exploit this vulnerability was use a non-HP chip on a third-party inkjet cartridge and reprogram it—injecting malware onto the chip. We wanted to know whose cartridge and whose chip the researcher used for the experiment, but Mr. Daniels told us that HP took a "hands-off approach to that." Mr. Daniels said HP told the researcher to just go on the open market and buy a third-party cartridge from whatever retailer the researcher preferred. "We didn't prescribe where he should buy from or what brand he should buy."

Ms. Albright explained that when the third-party cartridge with the infected chip was installed, the researcher was able to inject malware into the printer using that buffer overflow. She said, "Once you actually inject that malware into the memory of the device, you could essentially do whatever you want with this device." The white-hat hacker had "persistent access and control to the printer." She said the researcher could potentially capture information printed on the device and send that over the printer's network to the researcher's command and control server.

Mr. Daniels added that one interesting detail was that once the cartridge with the infected chip was inserted, "this became a persistent attack." He explained, "Even after the cartridge was removed, the malware remained on the printer in memory."

According to HP, the researcher found that the same vulnerability could not be exploited using original HP cartridges with original HP chips. Mr. Daniels said that is because HP's chips employed hardened security and are tamper resistant. "The researcher just could not achieve reprogramming HP chips," he said.

Fixing the Problems

HP told us that while the research was performed using an ink-based product, the vulnerabilities were discovered on a common firmware platform that spans across a broad range of printer families for both inkjet and LaserJet lineups.

Once the Bug Bounty researcher shared with HP how he was able to take control of a printer using malware on a third-party chip, HP sprang into action. Mr. Daniels said, "That's why we are really pleased with the Bug Bounty program is because we have been able to identify this vulnerability and fix it." So far, there's no evidence of this vulnerability "being exploited in the wild," said Mr. Daniels, although he added, "That's not to say that it hasn't. We just have no evidence of such an exploit." But he said that's the whole point of Bug Bounty—to find security flaws before they become a big problem.

Mr. Daniels said that HP has been rolling out new firmware for the past several weeks to address the issue. And, he added, it is security issues such as this that demonstrate why it is important for customers to keep printer firmware updated.

HP issued the following security bulletin about the issue to its customer support site: Certain HP Print Products – Potential Buffer Overflow, Remote Code Execution. There, HP explains this critical-level security issue is that certain HP printers "are potentially vulnerable to Buffer Overflow and/or Remote Code Execution." Affected products include a long list of DeskJet, ENVY, OfficeJet, Smart Tank, and Tango inkjet printers and all-in-ones; various LaserJet Pro laser printers and MFPs; and PageWide printers and MFPs. The security bulletin notes that the resolution to this security flaw is updating the printer firmware. HP says, "HP has provided firmware updates

© 2023 Actionable Intelligence

“Our view is anytime you use a non-HP unsecured third-party chip that’s field reprogrammable, your security risk profile increases.”

for potentially affected products listed in the table below. To obtain the updated firmware listed below, go to the HP Software and Driver Downloads, and then search for your printer model.”

We asked if given that HP has updated printer firmware to address this security flaw, whether that means HP has completely remedied the problem and that non-HP supplies with non-HP chips no longer pose a risk. Ms. Albright said that indeed the question might be, “Well now that we have fixed it, are we good to go with non-HP cartridges?” She said the answer is that third-party chips may still pose a risk. “We can never guarantee that every interface with a non-HP cartridge on our device will be free of bugs and security vulnerabilities,” she said.

Mr. Daniels said that following the Bug Bounty researcher’s findings about third-party reprogrammable chips and HP’s firmware fix, “Our cartridge security messages won’t change. But this experiment does move our cartridge security claims from a theoretical to now a demonstrated security risk. Our view is anytime you use a non-HP unsecured third-party chip that’s field reprogrammable, your security risk profile increases. There’s no doubt about it. You need to know the provenance of that cartridge and you need to know what’s on that code on the chip. And if you don’t trust it, why use it?”

It will be interesting to see if HP’s message resonates with end users. It’s not news that printers and MFPs, like any other device on a network, represent a security risk. Making sure that the data that flows into and out of these devices is secure has become essential to all IT professionals. There has been debate, however, not only over whether reprogrammable third-party chips pose a security risk but about whether or not it is essential from a security perspective to keep printer firmware up to date. HP has maintained that keeping the firmware in its printers updated is important for many reasons, including print quality and essential elements of the customer experience such as low on ink signals, authentication, and security. In contrast, third-party supplies makers and sellers routinely advise their customers not to update firmware because of the risk that a firmware update will prevent the use of third-party supplies. HP, however, clearly wants third-party supplies users to question that advice, update their firmware, and consider switching back to more secure HP cartridges with HP chips. Whether news that reprogrammable chips are hackable make security-minded users think twice before purchasing non-HP cartridges remains to be seen.

About Actionable Intelligence

Actionable Intelligence is the leading source for news, analysis, and research on the digital printer and MFP industry and the original and third-party consumables business. Actionable Intelligence provides clients with customized research and consulting, as well as up-to-date news and strategic analysis on Action-Intell.com, the industry’s leading destination site visited by tens of thousands of printer and supplies executives worldwide. Global printer OEMs, third-party supplies vendors, distributors, resellers, and a diverse mix of other companies rely on Actionable Intelligence to deliver timely and accurate information about the trends shaping the printer hardware and supplies markets. To learn more about Actionable Intelligence, visit www.action-intell.com.

© 2023 Actionable Intelligence