the Availability Digest

www.availabilitydigest.com
@availabilitydig

# HP Launches Bug Bounty Program for Printers

September 2018

HP is offering a bug bounty of up to $10,000 for flaws found in its printers. The vast majority of printers are attached to the same networks as local machines that could contain sensitive data. HP is concerned that a flaw in its printers could open the door to a company's entire network.

HP has the largest worldwide market share for printers sold.

Historically, Chief Security Information Officers (CSIOs) have not been involved in the purchase of printers. Unpatched or vulnerable printers have not been considered a serious threat. However, CISOs are now expecting more secure printers.

HP has made cybersecurity a priority for its printers. In doing so, HP is helping to support the valuable role that CISOs play in their organizations.

However, as more networking capabilities and cloud functions are introduced, printers are presenting a larger attack surface for hackers. Attackers have started to focus more on targeting endpoint devices such as printers in the past year. HP doesn't want one of it printers serving as a conduit for a larger attack on a company.

The bug bounty currently covers the HP Laser Jet Enterprise printers and the HP Page-Wide Enterprise edition printers. HP quietly launched the program in May 2018.

## What Is A Bug Bounty?

A bug bounty is a program offered by many websites and software developers by which individuals can receive compensation for reporting bugs. These programs allow developers to discover and resolve bugs before the general public is aware of them.

Bug bounty programs have been implemented by several major companies. Google, Apple, Facebook, Yahoo!, Microsoft, and many other companies use such programs. Several U.S. Agencies such as the Department of Defense have started using bug bounty programs. This is a policy shift from threatening computer security hackers with legal recourse to inviting them to participate as part of a comprehensive vulnerability disclosure framework.

## The History of Bug Bounties

Bug bounties have been used for years to help companies find defects in their systems. However, this is the first time that a bug bounty has been used for printers.

The first bug bounty program was launched in 1995 by Netscape, encouraging researchers to find bugs in its Netscape Navigator product. In 2004, Mozilla introduced a program to find defects in its Firefox product.

In 2010, Google introduced web applications as candidates for bug bounties. In 2011, Facebook joined with their own bug bounties, and Microsoft added bug bounties in 2015.

Now most major companies offer bug bounties of some sort or another to entice researchers to find defects in their systems.

## HP Seeks to Secure Its Printers via a Bug Bounty

Bug bounties allow a company to patch its products before the flaw becomes a target of nefarious hackers. Now HP is opening a new bug bounty program. It wants hackers to break into its printers.

With printers getting outfitted with more advanced functions, they are becoming a more attractive weak link in a network for hackers. Printers are appealing to hackers because of the tendency to leave printers unsecured.

Printers are now full-fledged computers. HP's printer bug bounty program is the first of its kind to patch one of the most dangerous security threats around. The program offers customers protection from attacks that are targeting both businesses and employees

HP's bug bounty program rewards those who spot security flaws in its products with serious money. Rewards range from $500 for a vulnerability with limited impact to $10,000 for a serious bug that could endanger a network.

HP has partnered with security firm Bugcrowd to launch the program. Bugcrowd will manage the new vulnerability disclosure award program for HP enterprise printers. A recent report from Bugcrowd showed a 21% increase in vulnerabilities discovered in printers. This indicates an increased risk for owning vulnerable printers, especially in the enterprise environment

The bug bounty program includes:

- Vulnerabilities found by researchers in the program are required to be reported to Bugcrowd.
- Bugcrowd will verify bugs and reward researchers based on the severity of the flaw up to $10,000.
- Reporting a vulnerability previously discovered by HP will be assessed, and a reward may be offered to researchers as a good-faith payment.

Shivaun Albright, HP chief technologist of print security, stated: "As we navigate an increasingly complex world of cyber threats, it's paramount that industry leaders leverage every resource possible to deliver trusted, resilient security from the firmware up. HP is committed to engineering the most secure printers in the world.

"Printers are increasing in storage and processing power. However, all the good security practices that are employed to protect PCs and other important nodes in the network are not being deployed with consistency to printers. We're seeing management in the deployment of printers leaving critical ports open. This makes it easy for attackers to remotely access the device."

According to Albright, HP wants to see if there are any defects it has missed. Any exposure point where there is an opportunity to input unexpected data is a potential area for hackers to target.

## Utilizing the Services of Hackers

Hacker-Powered Security is a technique that utilizes the external hacker community to find unknown security vulnerabilities and reduce cyber risk. These techniques include private bug bounty programs, public bug bounty programs, and vulnerability disclosure practices.

By using ethical hackers to find bugs via a bug-bounty program, organizations can identify high-value bugs faster. In the case of HP's printer bug bounty, the program encourages hackers to find defects in its enterprise systems.

## By Invitation Only

The current HP printer bug bounty program is not open to everyone. It is private and available by invitation only.

HP has selected 34 researchers to participate in the program.

## Other Bug Bounty Programs

Many companies are using bug bounties to improve their systems. United Airlines is one major company that is offering a bug bounty program. Others include Amazon, AOL, Apple, AT&T, Blackberry, Cisco, eBay, Facebook, GM, Google, Honeywell, IBM, Intel, LinkedIn, Mastercard, Microsoft, MIT, Motorola, Netflix, Oracle, Paypal, Red Hat, Sony, Starbucks, Tesla, Uber, and Ford. The fact that bug bounty programs are so popular among many large companies is a testament to how well they work.

Bug bounty programs are even used to help secure continuously available systems. Even though these systems are engineered to never fail, they can still have hidden bugs that can spell disaster if ever activated.

## Summary

Businesses are clamping down on the security of their software through bug bounty programs. If HP's new bug bounty program proves successful, we will likely see other manufacturers follow suite with bug bounty programs of their own.

## Acknowledgements

Information for this article was obtained from the following sources.

HP Launches Printer Bug Bounty Program, *Dark Reading*; July 31, 2018.
HP Announces First-Ever Bug Bounty Program for Printer Security, *CRN*; July 31, 2018.
HP Launches Industry's First Print Security Bug Bounty Program, *Press Ext HP.com.*
$10,000 for hacking HP printers: First bug bounty program for printer security, *CSO*; July 31, 2018.
HP Becomes the First Printer Maker to Launch a Bug Bounty, *Tom's Hardware*; July 31, 2018.
HP Launches First Bug Bounty Program for Printers, *Info Security*; September 6, 2018.
HP targets print security with bug bounty program, *ITP*; September 10, 2018.
HP launches printer bug bounty program, *Safety*; July 31, 2018.
The Hacker-Powered Security Report – Financial Services & Insurance Edition.
HP launches bug bounty program for printers, *Tech Radar*; July 31, 2018.
HP Launches $10,000 Bug Bounty for Printer, *Extreme Tech*; July 31, 2018.
Wikipedia.