bugcrowd

Executive Summary

Bugcrowd was engaged by HP Inc. to coordinate with researchers to perform security testing of an HP MFP477dw Multifunction Printer using a compatible, non-HP ink cartridge. The tests were completed in August 2022.

During this engagement several vulnerabilities in various components of the HP MFP477dw Multifunction Printer were discovered. When combined, these vulnerabilities provided a mechanism which allowed a malicious print cartridge to gain persistent code execution on the target printer's Linux operating environment as an administrative user ("root").

Due to the nature of these vulnerabilities, it was confirmed that a malicious print cartridge could be used to introduce malware onto the printer. This malware was able to persist on the printer after the malicious cartridge had been removed, and the printer rebooted.

A modified non-HP cartridge was provided to the HP security team, who confirmed that this malicious cartridge was able to successfully gain control of an unmodified retail HP MFP477dw Multifunction Printer when it was inserted into the printer.

The outcomes of this engagement demonstrate that a modified, or intentionally malicious, print cartridge could be utilized to successfully install malware into a target network through an HP printer, providing a pathway for an actor to gain a foothold in the network for additional post-exploitation activities, such as lateral movement and data theft.

To mitigate against potential attacks, HP printer users should be aware of their supply chain and purchase cartridges from trusted sources to ensure they are not modified or tampered with.

Details of the vulnerabilities and specific mode by which the malware was able to gain access will remain strictly confidential for security reasons.