  - Risk Management
  - Compliance
  - Privacy
  - Supply Chain
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Vulnerabilities

Hundreds of Thousands of Konica Printers Vulnerable to Hacking via Physical Access

By Eduard Kovacs on May 12, 2022

Share Tweet 推荐 0 RSS

Researchers at Atos-owned cybersecurity consulting firm SEC Consult analyzed Konica Minolta printers to determine what could be achieved by an attacker who has physical access to a device. The answer: a lot!

The analysis was conducted in late 2019 and it targeted Konica Minolta bizhub C3300i and C3350i multi-function printers (MFPs).

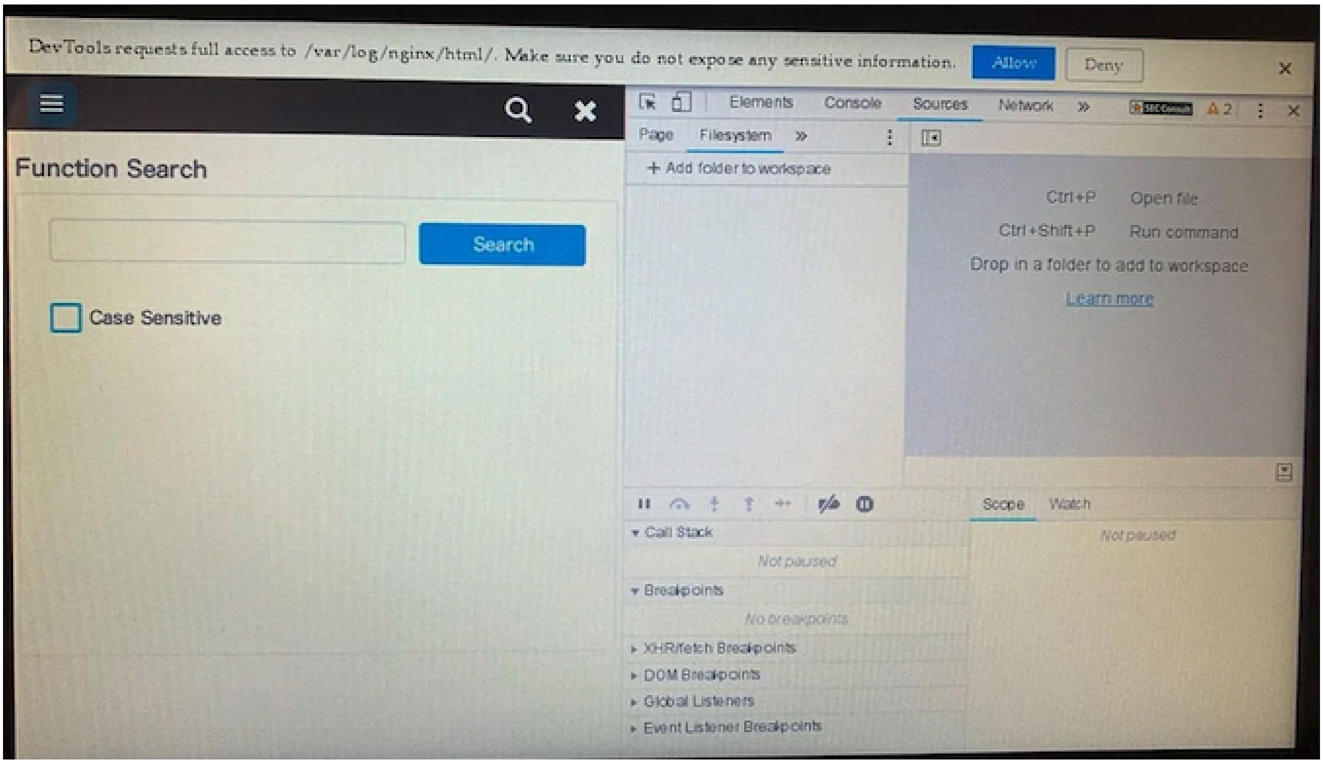
SEC Consult said the vendor was responsive and produced firmware and operating system patches in early 2020, but details are only being disclosed now because the COVID-19 pandemic prevented the delivery of the fixes to devices. While a remote firmware update mechanism is being rolled out, the patches in many cases need to be manually installed by a service technician.

SEC Consult found that an attacker who has physical access to the targeted device's touchscreen terminal could escape the sandbox and gain root access to the underlying operating system.

The analysis resulted in the discovery of three vulnerabilities. One of them, tracked as CVE-2022-29586, allows an attacker who can connect an external USB keyboard to the printer to escape the regular user interface displayed in the terminal. The researchers found that some sections of the interface were actually a Chromium browser running in "kiosk mode," which could be escaped by pressing the F12 key, which opens up the developer console.

Since this Chromium instance was running with root privileges — this issue has been assigned CVE-2022-29587 — an attacker could gain elevated permissions and abuse the developer console to read and write arbitrary files to the system. The files that could be accessed included files that stored administrator passwords in clear text (CVE-2022-29588).

SEC Consult showed that an attacker could have tampered with the touchscreen to display a website controlled by the attacker instead of the regular user interface. This could have been used to display fake login screens to phish domain credentials, or to automatically send a copy of printed or scanned files to a remote server controlled by the attacker.



DevTools requests full access to /var/log/nginx/html/. Make sure you do not expose any sensitive information.

The Japanese tech giant's investigation showed that the vulnerabilities impact 46 bizhub MFP models, as well as rebranded products offered by multiple unnamed companies. SEC Consult estimates that hundreds of thousands of printers around the world are affected — or at least they were affected at one point before patches were deployed. A list of impacted models is available in an advisory published on Thursday by SEC Consult.

In addition to providing patches, Konica Minolta recommends some mitigations, such as disabling the use of external USB keyboards. Another mitigating factor, as pointed out by SEC Consult, is that "Public User Access" needs to be enabled on the printer for the attack to be possible.

Related: Serious Vulnerability Exploited at Hacking Contest Impacts Over 200 HP Printers

Related: Xerox Quietly Patched Device-Bricking Flaw Affecting Some Printers

Related: Critical Vulnerability Found in More Than 150 HP Printer Models

Share Tweet 推荐 0 RSS