  - 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

1,000 Organizations Exposed to Remote Attacks by FileWave MDM Vulnerabilities

By Eduard Kovacs on July 25, 2022

Share Tweet 推荐 19 RSS

Vulnerabilities affecting a mobile device management (MDM) product from FileWave exposed many organizations to remote attacks, according to industrial cybersecurity firm Claroty.

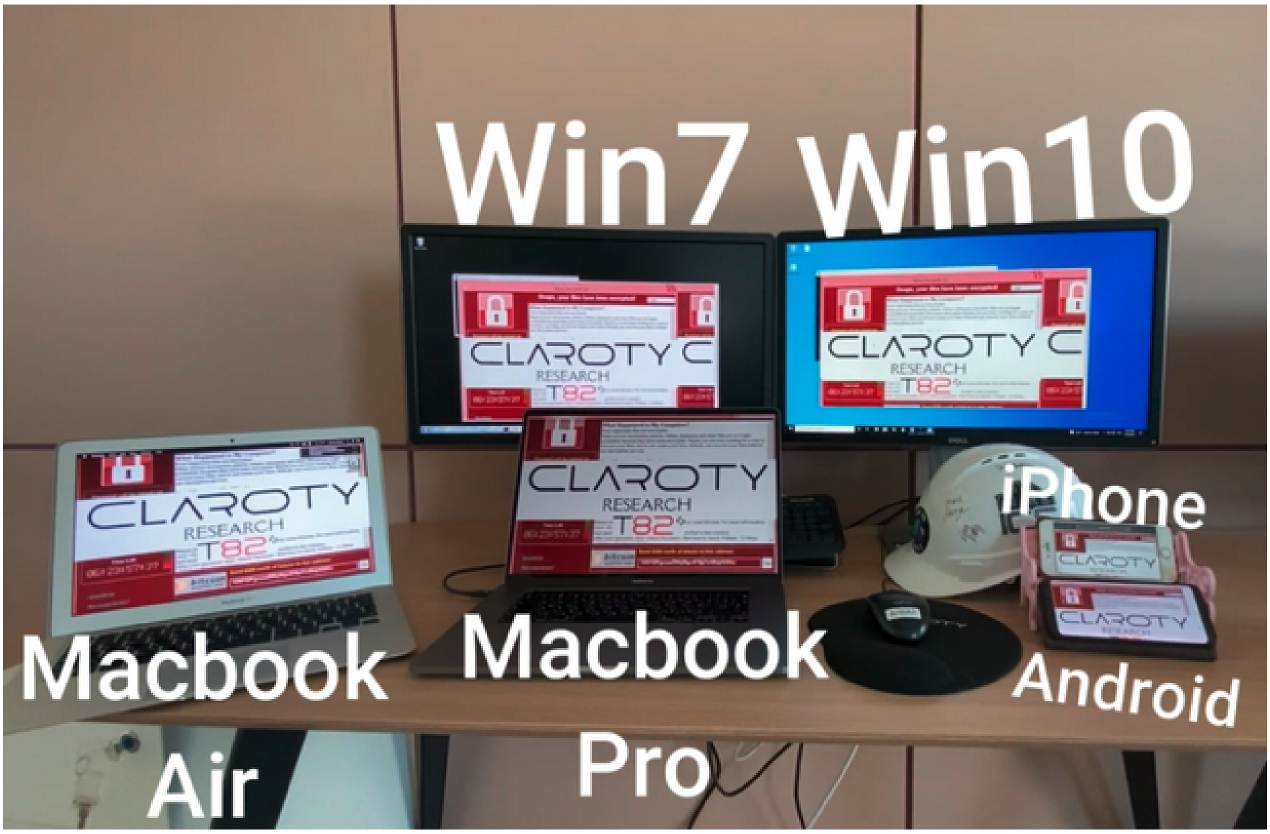
Claroty researchers discovered recently that the FileWave MDM product is affected by two critical security holes: an authentication bypass issue (CVE-2022-34907) and a hardcoded cryptographic key (CVE-2022-34906). The vendor quickly patched the flaws.

The authentication bypass vulnerability could allow a remote attacker to achieve “super_user” access and take full control of an internet-connected MDM instance. From there, the attacker could hack all devices managed using the FileWave product, including to steal sensitive information and deliver malware.

The researchers identified more than 1,100 internet-exposed instances of the vulnerable MDM server, including ones housed by corporations, educational institutions, government agencies, and SMBs.

This could have made these systems a tempting target for malicious actors looking to compromise many systems within an organization.

The cybersecurity firm conducted experiments to show how an attacker could exploit CVE-2022-34907 to obtain information about the managed devices and to install ransomware on each system, including macOS, iOS, Windows and Android devices.



“This exploit, if used maliciously, could allow remote attackers to easily attack and infect all internet-accessible instances managed by the FileWave MDM, below, allowing attackers to control all managed devices, gaining access to users’ personal home networks, organizations’ internal networks, and much more,” Claroty said in a blog post published on Monday.

FileWave patched the vulnerability in version 14.7.2, which it released earlier this month. According to the cybersecurity firm, the vendor has actively reached out to customers, urging them to patch affected systems.

Related: SureMDM Vulnerabilities Exposed Companies to Supply Chain Attacks

Related: Vulnerabilities Expose Thousands of MobileIron Servers to Remote Attacks

Related: Vulnerability Found in SimpleMDM Apple Device Management Solution

Share Tweet 推荐 19 RSS

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia’ s security news reporter. Eduard holds a bachelor’ s degree in industrial informatics and a master’ s degree in computer techniques applied in electrical engineering.
Previous Columns by Eduard Kovacs:
1,000 Organizations Exposed to Remote Attacks by FileWave MDM Vulnerabilities
Updated TSA Pipeline Cybersecurity Requirements Offer More Flexibility
Chrome Flaw Exploited by Israeli Spyware Firm Also Impacts Edge, Safari