SECURITYWEEK NETWORK:

- Cybersecurity News
- Infosec Island
- Virtual Events

Security Experts:

WRITE FOR US

SECURITY WEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe
- 2021 CISO Forum
- ICS Cyber Security Conference
- Contact

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Threat Intelligence
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance

- 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

PoC Exploit Released for macOS Gatekeeper Bypass

By Ionut Arghire on October 04, 2021

Rasmus Sten, a software engineer with F-Secure, has released proof-of-concept (PoC) exploit code for a macOS Gatekeeper bypass that Apple patched in April this year.

The PoC exploit targets CVE-2021-1810, a vulnerability that can lead to the bypass of all three protections that Apple implemented against malicious file downloads, namely file quarantine, Gatekeeper, and notarization.

This issue was found in the Archive Utility component of macOS Big Sur and Catalina and can be exploited using a specially crafted ZIP file. Successful exploitation requires for the attacker to trick the user into downloading and opening the archive to execute the malicious code within.

By exploiting the vulnerability, an attacker could execute unsigned binaries on macOS devices, even with Gatekeeper enforcing code signatures and without the user being alerted to the malicious code execution.

The vulnerability, Sten explains, is related to the manner in which the Archive Utility handles file paths. Specifically, the software engineer discovered that, for paths longer than 886 characters, the com.apple.quarantine extended attribute would no longer apply, resulting in a Gatekeeper bypass for the files.

While researching edge cases with long path filenames, Sten discovered that some macOS components behaved unexpectedly when the total path length reached a certain limit.

Eventually, Sten discovered that it was possible to create an archive with a hierarchical structure for which the path length was long enough so that Safari would call Archive Utility to unpack it and that Archive Utility would not apply the com.apple.quarantine attribute, but short enough to be browsable using Finder and for macOS to execute the code within.

“In order to make it more appealing to the user, the archive folder structure could be hidden (prefixed with a full stop) with a symbolic link in the root which was almost indistinguishable from a single app bundle in the archive root,” the researcher explains.

Sten, who also released a video demo of the exploit, has published PoC code that creates the archive with the path length necessary to bypass CVE-2021-1810, along with a symbolic link to make the ZIP file look normal.

The vulnerability was addressed with the release of macOS Big Sur 11.3 and Security Update 2021-002 for Catalina.

Related: **Apple Patches Security Bypass Vulnerability Impacting Macs With M1 Chip**

Related: **Hackers Can Exploit Apple AirTag Vulnerability to Lure Users to Malicious Sites**

Related: **Apple Deprecates Outdated TLS Protocols in iOS, macOS**

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:
Hackers Stole Cryptocurrency From Thousands of Coinbase Accounts
PoC Exploit Released for macOS Gatekeeper Bypass
Google Pledges $1 Million to Secure Open Source Program
Third-Party Identity Risk Provider SecZetta Raises $20.5 Million
Neiman Marcus Confirms Payment Cards Compromised in Data Breach

Tags:
NEWS & INDUSTRY Vulnerabilities