Attackers exploit an iTunes zeroday to install ransomware



reader comments

57 with 40 posters participating, including story author

Share this story

Attackers exploited a zeroday vulnerability in Apple's iTunes and iCloud programs to infect Windows computers with ransomware without triggering antivirus protections, researchers from Morphisec reported on Thursday. Apple patched the vulnerability earlier this week.

The vulnerability resided in the Bonjour component that both iTunes and iCloud for Windows relies on, according to a blog post. The bug is known as an unquoted service path, which as its name suggests, happens when a developer forgets to surround a file path with quotation marks. When the bug is in a trusted program—such as one digitally signed by a well-known

developer like Apple—attackers can exploit the flaw to make the program execute code that AV protection might otherwise flag as suspicious.

Morphisec CTO Michael Gorelik explained it this way:

> *As many detection solutions are based on behavior monitoring, the chain of process execution (parent-child) plays a major role in alert fidelity. If a legitimate process signed by a known vendor executes a new malicious child process, an associated alert will have a lower confidence score than it would if the parent was not signed by a known vendor. Since Bonjour is signed and known, the adversary uses this to their advantage. Furthermore, security vendors try to minimize unnecessary conflicts with known software applications, so they will not prevent this behaviorally for fear of disrupting operations.*

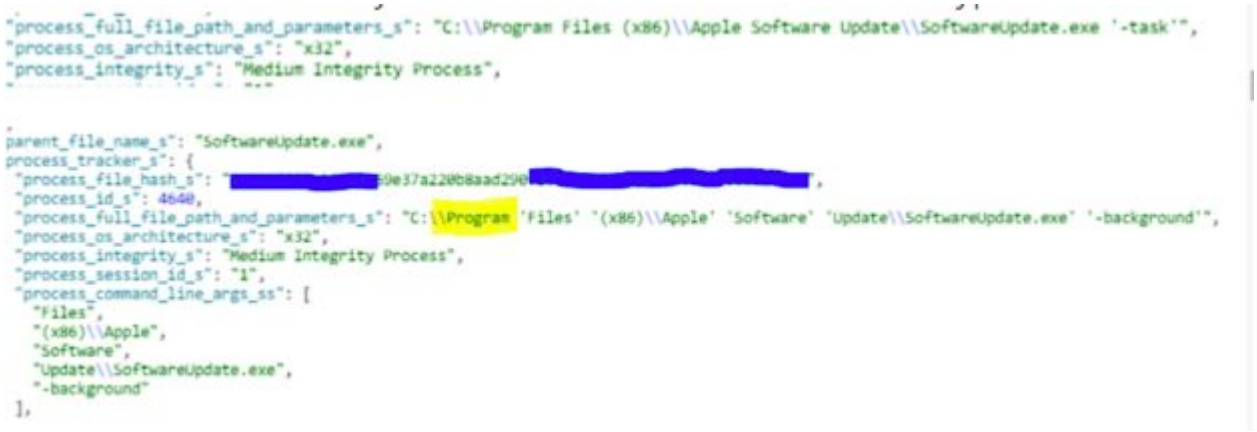
Unquoted path vulnerabilities have been found in other programs, including an Intel graphics driver, the ExpressVPN, and the Forcepoint VPN.

In August, Morphisec found attackers were exploiting the vulnerability to install ransomware called BitPaymer on the computers of an unidentified company in the automotive industry. The exploit allowed the attackers to execute a malicious file called "Program," which presumably was already on the target's network.

Gorelik continued:

> *Additionally, the malicious "Program" file doesn't come with an extension such as ".exe". This means it is likely that AV products will not scan the file since these products tend to scan only specific file extensions to limit the performance impact on the machine. In this scenario, Bonjour was trying to run from the "Program Files" folder, but because of the unquoted path, it instead ran the BitPaymer ransomware since*

it was named “Program”. This is how the zero-day was able to evade detection and bypass AV.



Gorelik said that Morphisec “immediately” notified Apple of the active exploit upon finding it in August. On Monday, Apple patched the vulnerability in both iTunes 12.10.1 for Windows and iCloud for Windows 7.14. Windows users who have either application installed should ensure the automatic updates worked as they’re supposed to. In an email, Gorelik said his company has reported additional vulnerabilities that Apple has yet to patch. Apple representatives didn’t respond to an email seeking comment for this post.

What’s more, anyone who has ever installed and later uninstalled iTunes should inspect their PCs to ensure Bonjour was also removed. That’s because the iTunes uninstaller doesn’t automatically remove Bonjour.

“We were surprised by the results of an investigation that showed the Bonjour updater is installed on a large number of computers across different enterprises,” Gorelik wrote. “Many of the computers uninstalled iTunes years ago while the Bonjour component remains silently, un-updated, and still working in the background.”

An aside: Gorelik described Bonjour as “a mechanism that Apple uses to deliver future updates.” Apple and many other resources, meanwhile, say it’s a service Apple applications use to find shared music libraries and other resources on a

local network. In an email, Gorelik said Bonjour serves both functions.

“Moreover in the specific attack, Bonjour was executing the SoftwareUpdate executable that is located under C:\\Program Files (x86)\\Apple Software Update\\SoftwareUpdate.exe, but instead they executed C:\\Program with the rest as parameters -> “C:\\Program ‘Files’ ‘(x86)\\Apple’ ‘Software’ ‘Update\\SoftwareUpdate.exe,'” he wrote. He went on to say that Apple developers “haven’t fixed all the vulnerabilities reported by us, only the one that was abused by the attackers.”

https://arstechnica.com/?p=1583285