55 New Security Flaws Found in Apple Software and Online Services

A team of cyber researchers observed several Apple online services for a few months and found at least 55 vulnerabilities, 11 of which are critical in severity.

The Flaws

The initial list of vulnerabilities includes 29 high severity, 13 medium severity, and 2 low severity ones. These threats when exploited could potentially allow an attacker to fully compromise both customer and employee applications, launch a worm that is capable of automatically hijacking a victim's iCloud account, retrieve vital source code for internal Apple projects, they could also fully compromise an industrial control warehouse software used by Apple, and take over the sessions of Apple employees with the capability of accessing management tools and sensitive resources.The flaws meant that an attacker could easily take over a user's iCloud account and steal all his personal data and files like photos, calendar information, videos, and documents, in addition to forwarding the same exploit to all of their contacts. The findings were reported by Sam Curry along with Brett Buerhaus, Ben Sadeghipour, Samuel Erb, and Tanner Barnes over a three-month period between July and September.

How did Apple respond?

After the vulnerabilities were disclosed to Apple, the iPhone maker took steps to patch some of the flaws within 1-2 business days, and the few others fixed within a span of 4-6 hours. So far, Apple has processed around 28 of the vulnerabilities with a total payout of $288,500 as part of its bug bounty program.

The critical bugs pointed out by the security team are as follows:

- Remote Code Execution via Authorization and Authentication Bypass
- Authentication Bypass via Misconfigured Permissions allows Global Administrator Access
- Command Injection via Unsanitized Filename Argument
- Remote Code Execution via Leaked Secret and Exposed Administrator Tool
- Memory Leak leads to Employee and User Account Compromise allowing access to various internal applications
- Vertica SQL Injection via Unsanitized Input Parameter
- Wormable Stored XSS allows Attacker to Fully Compromise Victim iCloud Account
- Full Response SSRF allows Attacker to Read Internal Source Code and Access Protected Resources
- Blind XSS allows Attacker to Access Internal Support Portal for Customer and Employee Issue Tracking
- Server Side PhantomJS Execution allows an attacker to Access Internal Resources and Retrieve AWS IAM Keys

One of the Apple domains that were impacted included the Apple Distinguished Educators site ("ade.apple.com") that allowed for an authentication bypass using a default password ("###INvALID#%!3"), thus permitting an attacker to access the administrator console and execute arbitrary code. Likewise, a flaw in the password reset process associated with an application called DELMIA Apriso, a warehouse management solution, made it possible to create and modify shipments, inventory information, validate employee badges, and even take full control over the software by creating a rogue user.

Recommendation

This article reminds us that no one or (no device) is 100% safe from cyber attacks. Everyone is vulnerable to attacks, yes, even high-end Apple devices and services. The best thing that you can do to protect your machine from these malicious attacks is making sure that you install regular software updates on your device. These software updates contain patches that fixes vulnerabilities in your system even before attackers find and exploit them.

References

https://www.scmagazine.com/home/security-news/vulnerabilities/facebook-starts-hacker-plus-loyalty-program-for-bug-bounties/

https://www.scmagazine.com/home/security-news/

https://www.theverge.com/2013/2/19/4005460/apples-computers-attacked-by-hackers-says-reuters

https://thehackernews.com/2020/10/apple-security.html

https://cyware.com/cyber-security-news-articles