

Apple pays \$288,000 to white-hat hackers who had run of company's network



Nick Wright. Used by permission.

reader comments

61 with 54 posters participating

Share this story

For months, Apple's corporate network was at risk of hacks that could have stolen sensitive data from potentially millions of its customers and executed malicious code on their phones and computers, a security researcher said on Thursday.

Sam Curry, a 20-year-old researcher who specializes in website security, said that, in total, he and his team found 55

vulnerabilities. He rated 11 of them critical because they allowed him to take control of core Apple infrastructure and from there steal private emails, iCloud data, and other private information.

The 11 critical bugs were:

- 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
- 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 attacker to Access Internal Resources and Retrieve AWS IAM Keys

Apple promptly fixed the vulnerabilities after Curry reported them over a three-month span, often within hours of his initial advisory. The company has so far processed about half of the vulnerabilities and committed to paying \$288,500 for them. Once Apple processes the remainder, Curry said, the total payout might surpass \$500,000.

“If the issues were used by an attacker, Apple would’ve faced massive information disclosure and integrity loss,” Curry said

in an online chat a few hours after posting a 9,200-word writeup titled *We Hacked Apple for 3 Months: Here's What We Found*. "For instance, attackers would have access to the internal tools used for managing user information and additionally be able to change the systems around to work as the hackers intend."

Curry said the hacking project was a joint venture that also included fellow researchers:

Two of the worst

Among the most serious risks were those posed by a stored cross-site scripting vulnerability (typically abbreviated as XSS) in JavaScript parser that's used by the servers at www.iCloud.com. Because iCloud provides service to Apple Mail, the flaw could be exploited by sending someone with an iCloud.com or Mac.com address an email that included malicious characters.

The target need only open the email to be hacked. Once that happened, a script hidden inside the malicious email allowed the hacker to carry out any actions the target could when accessing iCloud in the browser. Below is a video showing a proof-of-concept exploit that sent all of the target's photos and contacts to the attacker.

[embedded content]

Proof of Concept

Curry said the stored XSS vulnerability was wormable, meaning it could spread from user to user when they did nothing more than open the malicious email. Such a worm would have worked by including a script that sent a similarly crafted email to every iCloud.com or Mac.com address in the victims' contact list.

A separate vulnerability, in a site reserved for Apple Distinguished Educators, was the result of it assigning a

default password—“###INvALID#%!3” (not including the quotation marks)—when someone submitted an application that included a username, first and last name, email address, and employer.

“If anyone had applied using this system and there existed functionality where you could manually authenticate, you could simply login to their account using the default password and completely bypass the ‘Sign In With Apple’ login,” Curry wrote.

Eventually, the hackers were able to use bruteforcing to divine a user with the name “erb” and, with that, to manually log in to the user’s account. The hackers then went on to log in to several other user accounts, one of which had “core administrator” privileges on the network. The image below shows the Jive console, used to run online forums, that they saw.

With control over the interface, the hackers could have executed arbitrary commands on the Web server controlling the ade.apple.com subdomain and accessed internal LDAP service that stores user account credentials. With that, they could have accessed much of Apple’s remaining internal network.

Freaking out

In all, Curry’s team found and reported 55 vulnerabilities with the severity of 11 rated critical, 29 high, 13 medium, and two low. The list and the dates they were found are listed in Curry’s blog post, which is linked above.

As the list above makes clear, the hacks detailed here are only two of a long list Curry and his team were able to carry out. They performed them under Apple’s bug-bounty program. Curry’s post said Apple paid a total of \$51,500 in exchange for the private reports relating to four vulnerabilities.

As I was in the process of reporting and writing this post,

Curry said he received an email from Apple informing him that the company was paying an additional \$237,000 for 28 other vulnerabilities.

“My reply to the email was: ‘Wow! I am in a weird state of shock right now,’” Curry told me. “I’ve never been paid this much at once. Everyone in our group is still a bit freaking out.”

He said he expects the total payout could exceed \$500,000 once Apple digests all the reports.

An Apple representative issued a statement that said:

At Apple, we vigilantly protect our networks and have dedicated teams of information security professionals that work to detect and respond to threats. As soon as the researchers alerted us to the issues they detail in their report, we immediately fixed the vulnerabilities and took steps to prevent future issues of this kind. Based on our logs, the researchers were the first to discover the vulnerabilities so we feel confident no user data was misused. We value our collaboration with security researchers to help keep our users safe and have credited the team for their assistance and will reward them from the Apple Security Bounty program.

<https://arstechnica.com/?p=1712964>