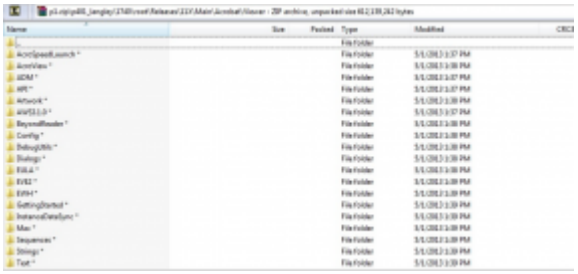
Adobe To Announce Source Code, Customer Data Breach

Published: 2013-10-22 · Archived: 2026-04-05 16:33:35 UTC

Adobe Systems Inc. is expected to announce today that hackers broke into its network and stole source code for an as-yet undetermined number of software titles, including its **ColdFusion** Web application platform, and possibly its **Acrobat** family of products. The company said hackers also accessed nearly three million customer credit card records, and stole login data for an undetermined number of Adobe user accounts.

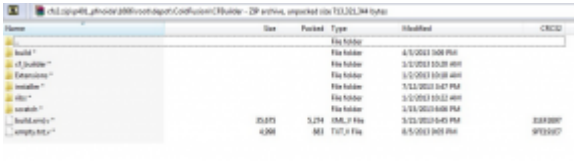


A screen shot of purloined source code stolen from Adobe, shared with the company by KrebsOnSec

KrebsOnSecurity first became aware of the source code leak roughly one week ago, when this author — working in conjunction with fellow researcher **Alex Holden**, CISO of Hold Security LLC — discovered a massive 40 GB source code trove stashed on a server used by the same cyber criminals believed to have hacked into major data aggregators earlier this year, including LexisNexis, Dun & Bradstreet and Kroll. The hacking team's server contained huge repositories of uncompiled and compiled code that appeared to be source code for ColdFusion and Adobe Acrobat.

Shortly after that discovery, KrebsOnSecurity shared several screen shots of the code repositories with Adobe. Today, Adobe responded with confirmation that it has been working on an investigation into a potentially broad-ranging breach into its networks since Sept. 17, 2013.

In an interview with this publication earlier today, Adobe confirmed that the company believes that hackers accessed a source code repository sometime in mid-August 2013, after breaking into a portion of Adobe's network that handled credit card transactions for customers. Adobe believes the attackers stole credit card and other data on approximately 2.9 million customers, and that the bad guys also accessed an as-yet-undetermined number of user names and passwords that customers use to access various parts of the Adobe customer network.



ColdFusion source code repository found on hacker's server.

Adobe said the credit card numbers were encrypted and that the company does not believe decrypted credit card numbers left its network. Nevertheless, the company said that later today it will begin the process of notifying affected customers — which include many Revel and Creative Cloud account users — via email that they need to reset their passwords.

In an interview prior to sending out a news alert on the company's findings, Adobe's Chief Security Officer Brad Arkin said the information shared by this publication "helped steer our investigation in a new direction." Arkin said the company has undertaken a rigorous review of the ColdFusion code shipped since the code archive was compromised, and that it is confident that the source code for ColdFusion code that shipped following the incident "maintained its integrity."

"We are in the early days of what we expect will be an extremely long and thorough response to this incident," Arkin said. The company is expected to publish an official statement this afternoon outlining the broad points of its investigation so far.

Arkin said Adobe is still in the process of determining what source code for other products may have been accessed by the attackers, and conceded that Adobe Acrobat may have been among the products the bad guys touched. Indeed, one of the screen shots this publication shared with Adobe indicates that the attackers also had access to Acrobat code, including what appears to be code for as-yet unreleased Acrobat components (see screen grab above).

"We're still at the brainstorming phase to come up with ways to provide higher level of assurance for the integrity of our products, and that's going to be a key part of our response," Arkin said. He noted that the company was in the process of looking for anomalous check-in activity on its code repositories and for other things that might seem out of place.

"We are looking at malware analysis and exploring the different digital assets we have. Right now the investigation is really into the trail of breadcrumbs of where the bad guys touched."

The revelations come just two days after KrebsOnSecurity published a story indicating that the same attackers apparently responsible for this breach were also involved in the intrusions into the networks of the National White Collar Crime Center (NW3C), a congressionally-funded non-profit organization that provides training, investigative support and research to agencies and entities involved in the prevention, investigation and prosecution of cybercrime. As noted in that story, the attackers appear to have initiated the intrusion into the NW3C using a set of attack tools that leveraged security vulnerabilities in Adobe's ColdFusion Web application server.

While Adobe many months ago issued security updates to plug all of the ColdFusion vulnerabilities used by the attackers, many networks apparently run outdated versions of the software, leaving them vulnerable to compromise. This indeed may have also been the vector that attackers used to infiltrate Adobe's own networks; Arkin said the company has not yet determined whether the servers that were breached were running ColdFusion, but acknowledged that the attackers appear to have gotten their foot in the door through "some type of out-of-date" software.

Stay tuned for further updates on this rapidly-moving story.

Update 4:38 p.m. ET: Adobe has released a statement about these incidents here and here. A separate customer security alert for users affected by this breach is here. Also, in a hopefully unrelated announcement, Adobe says it will be releasing critical security updates next Tuesday for Adobe Acrobat and Adobe Reader.

Update, Oct. 5, 4:35 p.m. ET: Rakshith Naresh, a product manager at Adobe, said in a Tweet yesterday that the breach did not involve ColdFusion vulnerabilities.

Update, Oct. 9, 12:50 p.m. ET: Naresh's Tweet stating that the breach didn't involve ColdFusion servers was deleted at some point. I followed up with Adobe via email: An Adobe spokesperson said the company's investigation is still ongoing, and that "at this time we have not identified the initial attack vector to include or exclude a ColdFusion server."
