ASSIGNMENT 01- REAL WORLD INCIDENT

Name : Rahul Goel
Reg No : RA1911030010094
Section : O2

ADOBE HACK IN 2013

Network Penetration

"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."

"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."

Timeline

1.Recon
2.Weaponisation
3.Delivery
4.Exploitation
5.Installation
6.Command and Control, Actions on Objectives

Vulnerabilities

Vulnerability #1

Adobe has released updates for Adobe Premiere Rush for
Windows and macOS. This update addresses
a moderate vulnerability. Successful exploitation could lead to privilege escalation in the context of the current user.

Vulnerability #2
Adobe has released an update for Adobe Illustrator 2022 and Adobe Illustrator 2021. This update
resolves critical, important and moderate vulnerabilities that
could lead to privilege escalation, application denial
of service, and memory leak

Vulnerability #3
Adobe has released an update for Photoshop for
Windows and macOS. This update resolves
a critical vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.

Vulnerability #4
Adobe has released an update f or Adobe After Effects for Wind owns and macOS. This update an addresses a critical security vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.

Costs

Adobe will pay just $1 million to settle a lawsuit filed by 15 state attorneys general over its huge 2013 data breach that exposed payment records on approximately 38 million people. In other news, the 39- year-old Dutchman responsible for coordinating an epic, weeks-long distributed denial-of-service
attack against anti-spam provider Spamhaus in 2013 will avoid any jail time for his crimes thanks to a court ruling in Amsterdam this week.

Prevention

“Adobe discovered that one or more unauthorised intruder(s) had compromised a public-facing web server and used it to access other servers on Adobe’s network, including areas where Adobe stored consumer data,” the statement from Healey’s office reads. “The intruder(s) ultimately stole consumer data from Adobe’s servers, including encrypted payment card numbers and expiration dates, names, addresses, telephone numbers, e-mail addresses, usernames (Adobe IDs), and passwords associated with the usernames.”