MOVEit Hacks: Stories and lessons learned

Daniel Iwugo
Published in InfoSec Write-ups
4 min read · Jul 9

MOVEit by Progress

The MOVEit file transfer software has been in the news lately as being a point of compromise for many organisations within the past few weeks. The vulnerability

stems from an SQL injection, which could lead to Remote Code Execution if carried out properly.

The last time the cybersecurity community saw such a series of attacks was with the Apache Log4j vulnerability, which affected thousands of servers worldwide. The MOVEit transfer software severity level is no different, as it is used to transfer files within and out of organisations securely (until recently that is).

On June 1, Bleeping Computer reported that hackers were exploiting a new critical zero-day vulnerability in the MOVEit Transfer software to steal data from organizations. The vulnerability affected HTTP and HTTPS transfers and Progress advised the ports to be blocked.

The following day, Mandiant released a blog post, informing that the vulnerability had been exploited as early as May 27. However, Security week reported that it had been around as early as July 2021.

Mandiant initially attributed a campaign exploiting the vulnerability to FIN11. However, on June 5, the Cl0P ransomware group announced they were responsible for attacks on infrastructure for the purpose of data theft.

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

Cl0p's Announcement ¦Credit: Mandiant

Progress said they had patched the vulnerability on May 31, but that was just the beginning of the unfortunate series of events that followed. The following took place within the days ahead.

Nova Scotia

A lighthouse in Nova Scotia ¦ Credit: Pixabay

On June 3, Nova Scotia had announced that there was a privacy breach affecting as many as 100,000 people were affected. The MOVEit vulnerability was used to steal personal information of employees of Nova Scotia Health, IWK Health Care and the public service.

BBC, British Airways and Boots

BBC News ¦ Credit: Bret Jordan

On June 5, the BBC reported that British Airways, Boots, Aer Lingus, Zellis, and them, were also hacked using the MOVEit vulnerability. The report mentioned that data stolen from the BBC included staff identification numbers, birth dates, and national insurance numbers. On the other hand, British Airways staff were warned that some of their bank details were probably stolen.

CISA and the FBI

Luckily, these guys weren't hacked. But on June 7th, CISA and the FBI, released a joint advisory for the vulnerability while attributing its exploitation to the Cl0p ransomware group.

Ofcom, Transport for London and Ernst & Young

A London Bus ¦ Credit: Gotta Be Worth It

On June 12, the BBC reported that Ofcom, Transport for London, and Ernst & Young had joined the list of known victims. Personal information of 412 employees was downloaded during the attack but no payroll data was affected.

US Department of Energy, Oregon and Louisiana

Parked Trucks ¦ Credit: Kevin Bidwell

On June 15, the CNN reported that the US department of energy joined the hitlist. The very next day, over 3.5 million people had their personal data compromised in an attack that targeted Oregon and Louisiana. The attack also compromised over 6 million records containing driver's licenses and vehicle registration.

More Vulnerabilities

As of 7th July, 2023, MOVEit has had 4 critical vulnerabilites. Today, The Hacker News reported that another SQL injection vulnerability was discovered in the software, and MOVEit has made the necessary patches to all of them. But with all this chaos, how are people and organisations supposed to protect themselves?

Mitigations

According to CISA, some of the ways to protect yourself include:

1. Use security software/antivirus
2. Update your applications and OS
3. Keep backups of your files on offline storage devices

4. Have strong passwords on all your devices and accounts (‘qwerty’ does not suffice 🔑)
5. Use Multi-factor authentication when possible

The full advisory can be found here if you want a closer look 👀.

If you liked this article, don’t forget to clap, leave a comment or hit the follow button. You could also subscribe to my email list to get more content like this. Always ensure to keep yourself safe in the online jungle and see you in the next one 🙃.

Moveit Transfer | Cyberattack | Cybercrime | Cl0p | Mercurysnotes

Edit profile

Written by Daniel Iwugo

120 Followers · Writer for InfoSec Write-ups

Just another guy fascinated by the world of Hacking, Cybersecurity and the Internet.

More from Daniel Iwugo and InfoSec Write-ups