EXPLOITATION D'UNE VULNÉRABILITÉ AFFECTANT MOVEIT PAR LE GROUPE CYBERCRIMINEL CLOP

5 juillet 2023

Contexte

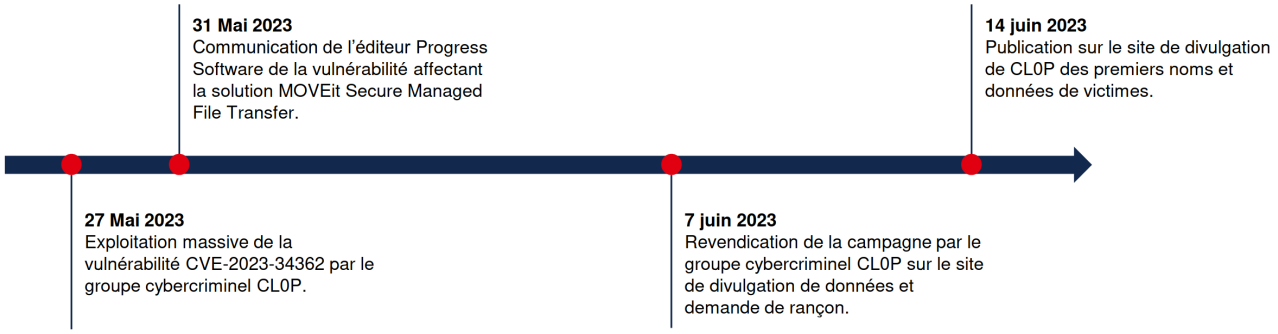

FIG. 1. – Chronologie de l'exploitation de la vulnérabilité MOVEit par CL0P

La vulnérabilité CVE-2023-34362 affectant la solution MOVEit Secure Managed File Transfer a été communiquée sur le site de l'éditeur PROGRESS SOFTWARE le 31 mai 2023 [1, 2]. L'exploitation massive de cette vulnérabilité par un groupe cybercriminel a été observée à partir du 27 mai 2023 [1, 3, 4]. Une fois la vulnérabilité exploitée, les cybercriminels ont exfiltré des données à des fins d'extorsion.

Le 7 juin, cette campagne a été revendiquée par le groupe cybercriminel CL0P sur son site de divulgation de données.

À partir du 14 juin, les noms de différentes victimes de cette campagne et des extraits de données exfiltrées ont été publiés sur le site du groupe CL0P. En plus de menacer de publier ces données, les opérateurs du groupe proposent de les mettre en vente. Elles pourraient alors être utilisées pour mener d'autres attaques.

Plus de 80 noms de victimes ont été publiés sur le site de divulgation de CL0P, dont trois entreprises françaises. D'autres entreprises internationales disposant de filiales françaises ont également été ciblées par cette campagne. Des données de clients et de prestataires des entreprises victimes peuvent être également présentes dans les données exfiltrées.

1. Un groupe cybercriminel mature et sophistiqué

Cette campagne d'exploitation de la vulnérabilité MOVEit est attribuée au mode opératoire FIN11 par MANDIANT, également nommé LACE TEMPEST par MICROSOFT.

Ce mode opératoire, associé au rançongiciel CL0P, mène des opérations de *Big Game Hunting* [1] et a recours à la double extorsion. Cependant, lors de l'exploitation de la vulnérabilité affectant MOVEit Transfer, aucun rançongiciel n'a été déployé, probablement afin d'exploiter rapidement et simultanément toutes les victimes et d'éviter une détection prématurée.

Commentaire : Le Panorama de la menace 2021, publié par l'ANSSI, faisait déjà état de cette tendance de chantage à la divulgation des données sans déploiement de rançongiciel [5].

L'exploitation de la vulnérabilité CVE-2023-34362, détaillée notamment par l'éditeur de cybersécurité HUNTRESS [3], était suivie par le déploiement d'un *webshell* nommé **LEMURLOOT** par MANDIANT [4]. Ce *webshell* a été conçu spécifiquement pour cette exploitation et reflète les capacités importantes des attaquants. L'orchestration nécessaire à l'exploitation massive de la vulnérabilité illustre également la maturité de ce groupe cybercriminel et les moyens mis en œuvre avec l'utilisation d'une *zero-day*.

1. dont l'objectif est de cibler de grandes organisations pour leur extorquer d'importantes sommes d'argent.

Plusieurs exploitations de vulnérabilités sur des solutions de transfert de fichiers sécurisé ont été attribuées à ce groupe dans les dernières années, notamment Accellion File Transfer Applicance (FTA) en 2020 [6], Serv-U en 2021 [7, 8] et GoAnywhere MFT en 2023 [9, 10].

L'exploitation de vulnérabilités dans des solutions de transfert de fichiers sécurisé ne semble pas aléatoire. Ces applications exposées sur Internet sont utilisées par de grandes organisations. Elles permettent un accès immédiat à de nombreux documents, notamment des données d'intérêt. Par ailleurs, la recherche de vulnérabilités par la communauté de chercheurs en cybersécurité sur ces solutions semble limitée. Il est probable que ce groupe ait développé une expertise et cherche à exploiter d'autres applications de cette catégorie de solutions dans le cadre de campagnes s'apparentant à des attaques par *supply chain*. D'autres solutions similaires pourraient être également ciblées à l'avenir : Globalscape EFT, Pro2col Coviant Diplomat MFT, Axway MFT, Cleo MFT, Oracle MFT, Citrix ShareFile MFT, Adobe Send & Track MFT, LeapFile, IBM MFT, Accellion Kiteworks, ou Zoho WorkDrive [11].

L'activité du groupe depuis la fin de l'année 2022 ne s'est pas limitée à l'exploitation de vulnérabilités sur des solutions de transfert de fichiers sécurisé. En effet, d'autres campagnes d'attaques, telles que la compromission initiale par **Raspberry Robin**, l'exploitation d'une vulnérabilité sur le logiciel de gestion d'impression PaperCut, ou des campagnes d'hameçonnage ont également imputées au groupe LACE TEMPEST par Microsoft [12, 13, 14].

Le groupe cybercriminel CL0P est plus largement imputé au groupe cybercriminel TA505 [13, 15], observé depuis 2014, dont les opérations ont été détaillées par l'ANSSI en 2020 [16].

2. Vulnérabilités MOVEit identifiées et correctifs à appliquer

Suite à l'exploitation de la vulnérabilité CVE-2023-34362 [1, 2], l'éditeur Progress Software a successivement déclaré deux autres vulnérabilités critiques, respectivement référencées CVE-2023-35036 et CVE-2023-35708 [17, 18]. Pour celles-ci, l'éditeur n'a cependant pas connaissance de campagnes d'exploitation. Ces vulnérabilités, toutes de type injection SQL affectent la solution MOVEit Secure Managed File Transfer et permettent à un attaquant non authentifié l'accès, l'élévation de privilèges, l'extraction ou la modification de la base de données du produit.

Dans tous les cas, il est nécessaire d'appliquer, d'une part, les mesures de remédiation documentées dans le premier avis de l'éditeur afin de vérifier si le serveur a été compromis [1]. Des indicateurs de compromission sont fournis par Progress Software et Rapid7 [1, 19]. D'autre part, l'éditeur fournit un correctif cumulatif en date du 15 juin 2023. En cas de difficultés pour déployer le correctif, les mesures de contournement énoncées dans le dernier avis de l'éditeur devront être appliquées [18].

L'éditeur propose deux façons d'appliquer les correctifs :

- la première consiste en le remplacement des bibliothèques (*DLL*) incriminées ;
- la seconde consiste en l'installation d'une version complète du produit (*Full Installer*).

Pour ces deux options, la liste des versions corrigeant les vulnérabilités est spécifiée dans le dernier avis de l'éditeur [18].

Par ailleurs, dans le cadre d'une installation par *DLL*, l'éditeur indique :

- de ne laisser aucune ancienne version de ces fichiers *DLL* sur le système. Ces derniers doivent être complètement supprimés, et pas seulement renommés ;
- que lors de l'arrêt des services MOVEit Transfer, il est nécessaire d'arrêter également les services IIS (*World Wide Web Publishing Services*) pour remplacer avec succès les anciennes *DLL*. Une fois les nouveaux fichiers copiés dans leurs destinations respectives, il est nécessaire de redémarrer les services MOVEit Transfer et IIS.

En cas de suspicion de compromission, il est recommandé de continuer les investigations (voir Les bons réflexes en cas d'intrusion sur un système d'information).

A. Bibliographie

[1] PROGRESS. *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362) - Progress Community*. 16 juin 2023.
URL : https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.

[2] CERT-FR. *Bulletin d'actualité CERTFR-2023-ACT-025*. 12 juin 2023.
URL : https://www.cert.ssi.gouv.fr/actualite/CERTFR-2023-ACT-025/.

[3] HUNTRESS. *MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response*. 1er juin 2023.
URL : https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response.

[4] MANDIANT. *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*. 2 juin 2023.
URL : https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

[5] CERT-FR. *Panorama de La Menace Informatique 2021*. 9 mars 2022.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-002/.

[6] MANDIANT. *Threat Actors Exploit Accellion FTA for Data Theft and Extortion*. 22 février 2021.
URL : https://www.mandiant.com/resources/blog/accellion-fta-exploited-for-data-theft-and-extortion.

[7] NCC GROUP. *TA505 Exploits SolarWinds Serv-U Vulnerability (CVE-2021-35211) for Initial Access*. 8 novembre 2021.
URL : https://research.nccgroup.com/2021/11/08/ta505-exploits-solarwinds-serv-u-vulnerability-cve-2021-35211-for-initial-access/.

[8] Alex Clinton-Tasha CROWDSTRIKE. *How Falcon Complete Stopped a SolarWinds Serv-U Exploit Campaign*. 21 octobre 2021.
URL : https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-solarwinds-serv-u-exploit-campaign/.

[9] HUNTRESS. *Investigating Intrusions From Intriguing Exploits*. 8 février 2023.
URL : https://www.huntress.com/blog/investigating-intrusions-from-intriguing-exploits.

[10] BLEEPING COMPUTER. *Clop Ransomware Claims It Breached 130 Orgs Using GoAnywhere Zero-Day*. 10 février 2023.
URL : https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/.

[11] @BUSHIDOTOKEN. *Which MFT Could #CL0P Target Next ?* 27 juin 2023.
URL : https://twitter.com/BushidoToken/status/1673721317634326530.

[12] MSTIC. *Raspberry Robin Worm Part of Larger Ecosystem Facilitating Pre-Ransomware Activity*. 27 octobre 2022.
URL : http://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/.

[13] MICROSOFT THREAT INTELLIGENCE [@MSFTSECINTEL]. *Lace Tempest (DEV-0950) Is a Clop Ransomware Affiliate That Has Been Observed Using GoAnywhere Exploits and Raspberry Robin Infection Hand-Offs in Past Ransomware Campaigns. The Threat Actor Incorporated the PaperCut Exploits into Their Attacks as Early as April 13.* 26 avril 2023.
URL : https://twitter.com/MsftSecIntel/status/1651346656657305603.

[14] THE DFIR REPORT. *A Truly Graceful Wipe Out*. 12 juin 2023.
URL : https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/.

[15] CISA. *#StopRansomware : CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*. 7 juin 2023.
URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[16] CERT-FR. *Évolution de l'activité Du Groupe Cybercriminel TA505 – CERT-FR*. 22 juin 2020.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-006/.

[17] PROGRESS. *MOVEit Transfer Critical Vulnerability – CVE-2023-35036 (June 9, 2023) - Progress Community*. 9 juin 2023.
URL : https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-2023-35036-June-9-2023.

[18] PROGRESS. *MOVEit Transfer Critical Vulnerability – CVE-2023-35708 (June 15, 2023) - Progress Community*. 15 juin 2023.
URL : https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023.

[19] RAPID7. *Observed Exploitation of MOVEit Transfer Vulnerability CVE-2023-34362 | Rapid7 Blog*. 1er juin 2023.
URL : https://www.rapid7.com/blog/post/2023/06/01/rapid7-observed-exploitation-of-critical-moveit-transfer-vulnerability/.

5 juillet 2023

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
cert.ssi.gouv.fr / cert-fr@ssi.gouv.fr