Jun 10 2023

NETMANAGEIT

Intelligence Report

Critical Vulnerability in Progress MOVEit Transfer: Technical Analysis and Recommendations

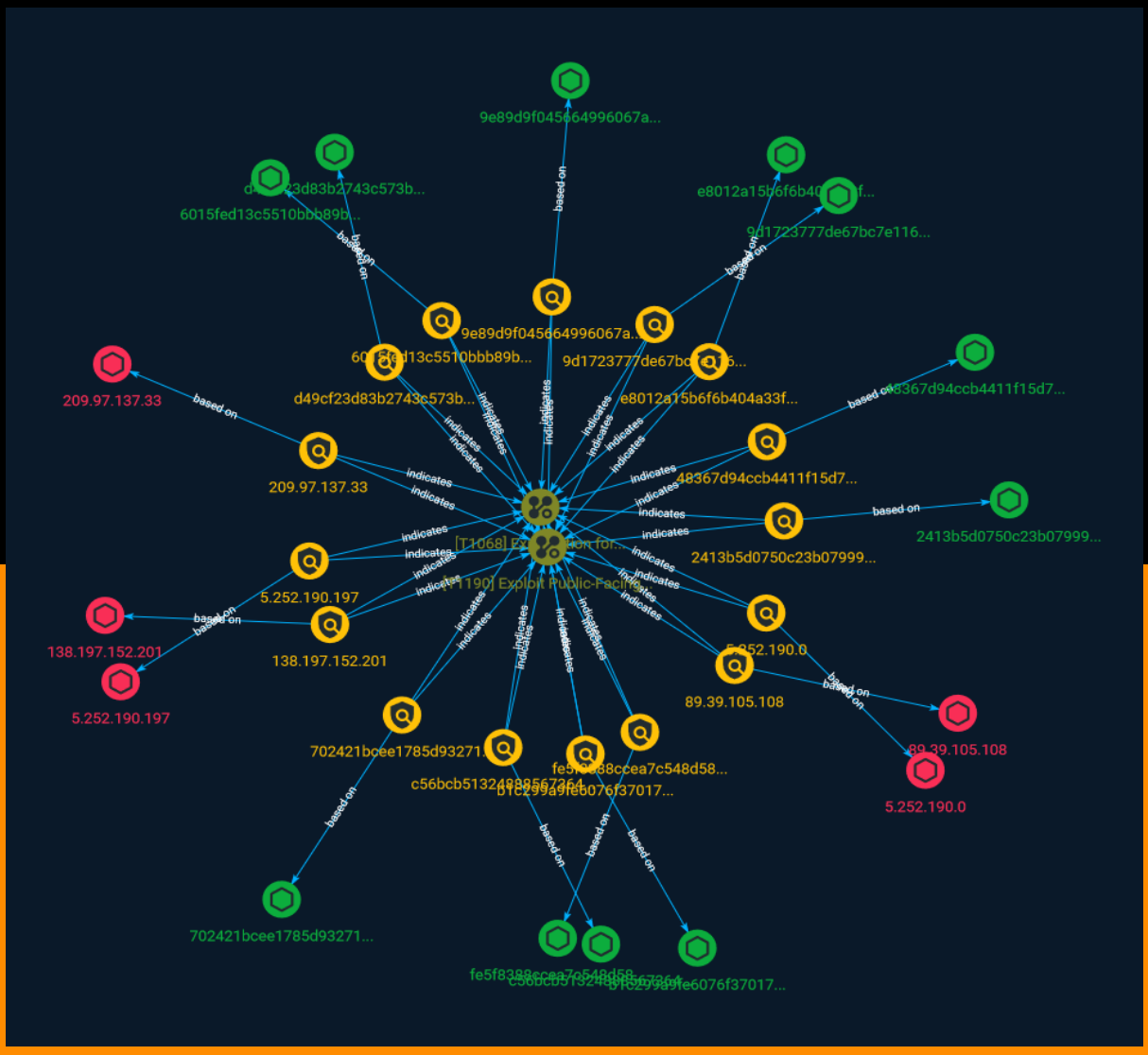

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers at TrustedSec have published a new blog on the analysis and exploration of a critical vulnerability in the MOVEit Transfer product. Attackers are deploying the human2.aspx backdoor, which allows obtaining a list of all folders, files, and users within MOVEit, downloading any file within MOVEit, and escalating privileges.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name
Exploitation for Privilege Escalation
ID
T1068
Description
Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a

compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

Exploit Public-Facing Application

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Indicator

Name
2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5']
Name
702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0']
Name

9e89d9f045664996067a05610ea2b0ad4f7f502f73d84321fb07861348fdc24a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9e89d9f045664996067a05610ea2b0ad4f7f502f73d84321fb07861348fdc24a']

Name

89.39.105.108

Description

CC=NL ASN=AS49981 WorldStream B.V.

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.39.105.108']

Name

5.252.190.197

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.252.190.197']

Name

e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e']

Name

b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272']

Name

d49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195']

Name

5.252.190.0

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.252.190.0']

Name

138.197.152.201

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC7MK7ZGMFUS/DuvrLJoXk7nFRS2uSjoW5es5Z56RGtDuA5 KL3MKq2btnH9X5xJH81EAEvwSsU78RKAFbibD5l9Z4/T6dsv+BbNGmRnCyr6SGo9X1uMO2sq9fcp +y5kAgRu7ZaSlSz5lDAMlZbqDbsgqPCxmJ2XpcPdlQdnmezoeFt3N1/P6OyMv+66kLjWadk1aGZz 7Ip5euQX/Djcpi30lD3I82WfxMqveSFvZJ6UtMf1v7PmVdjOluSTMzHyYq4Z+kHaz2naAqbg8mO2 mHpcRmDsDYxbikax6aJ6PN+uKFB/k/tx0NMZe9D6HHjiBNk9ucAmn1y7t50Wu8NKaIdt Fingerprint: 00:52:53:52:fe:3f:ee:f7:ed:66:35:a0:ad:c6:68:be Kex Algorithms: diffie-hellman-group1-sha1 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519

Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Tue, 31 Jan 2023 05:07:00 GMT Server: Apache/2.4.29 (Ubuntu) Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, OPTIONS Vary: Cookie,Accept-Encoding Set-Cookie: sessionid=7f8pabhljrwwa022y6fbs6uzbdfdh9os; httponly; Path=/ Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '138.197.152.201']

Name

9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead']

Name

fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f

Description

SHA256 of a85299f78ab5dd05e7f0f11ecea165ea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f']

Name

209.97.137.33

Description

CC=GB ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.97.137.33']

Name

48367d94ccb4411f15d7ef9c455c92125f3ad812f2363c4d2e949ce1b615429a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '48367d94ccb4411f15d7ef9c455c92125f3ad812f2363c4d2e949ce1b615429a']

Name

c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4']

Name

6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d']

StixFile

Value
2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5
b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272
fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f
c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4
702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0
48367d94ccb4411f15d7ef9c455c92125f3ad812f2363c4d2e949ce1b615429a
9e89d9f045664996067a05610ea2b0ad4f7f502f73d84321fb07861348fdc24a
e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e
d49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195
9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead
6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d

IPv4-Addr

Value
89.39.105.108
5.252.190.197
138.197.152.201
5.252.190.0
209.97.137.33

External References

- https://www.trustedsec.com/blog/critical-vulnerability-in-progress-moveit-transfer-technical-analysis-and-recommendations/
- https://otx.alienvault.com/pulse/64799ae9f3db8938cdc5ad23