Jun 10 2023

NETMANAGEIT

Intelligence Report

Trustwave Action Response: Zero Day Exploitation of MOVEit (CVE-2023-34362)

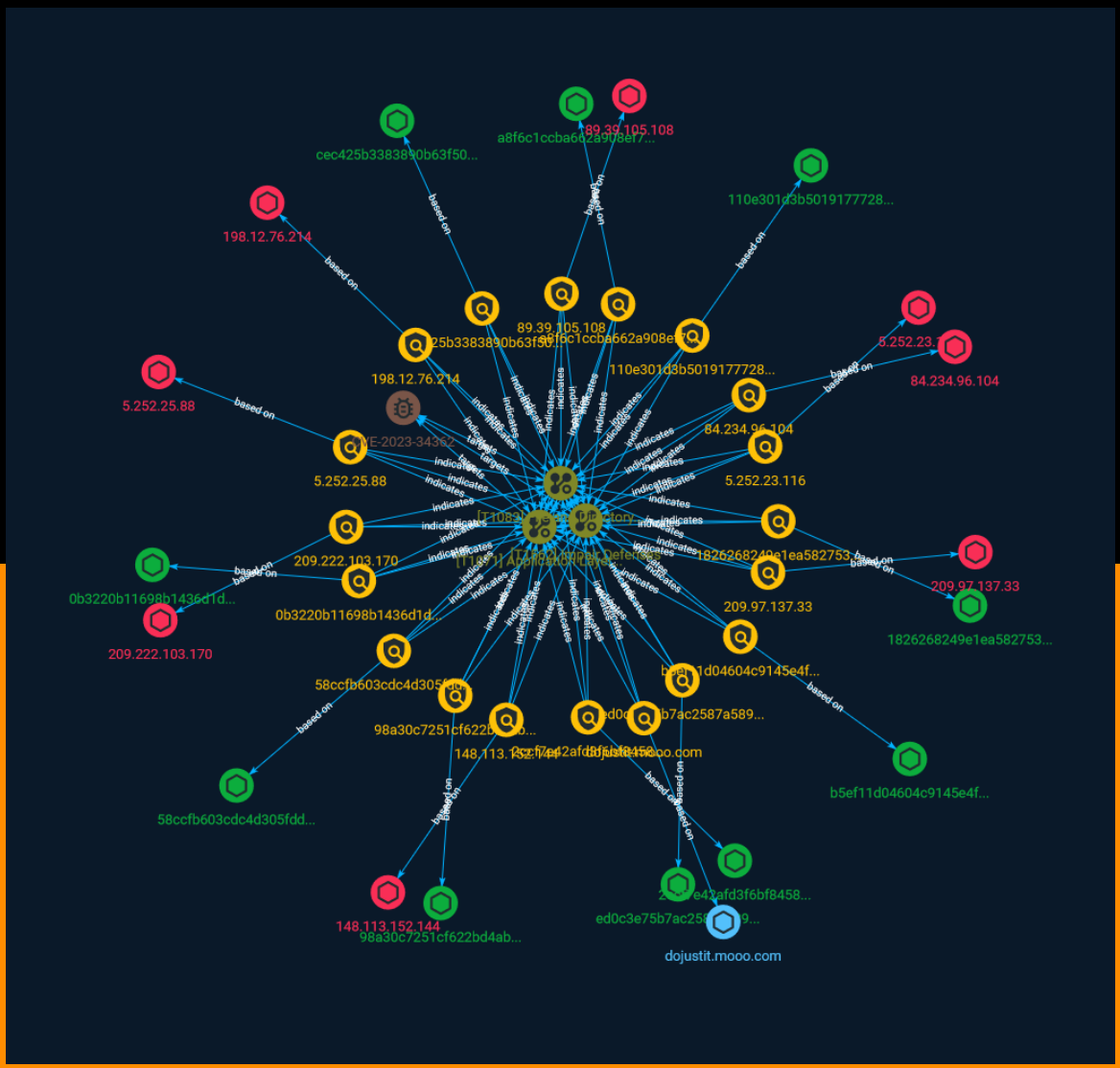

Table of contents

Overview

Entities

Observables

External References

Overview

Description

On May 31, threat actors were discovered targeting a critical zero day in MOVEit Transfer software resulting in escalated privileges and unauthorized data access. The vulnerability being exploited is an SQL injection and has since been patched. Resources links, including one for the patch, are at the bottom of this post.

Confidence

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

15 / 100

Attack-Pattern

Name
Impair Defenses
ID
T1562
Description
Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out of a computer or stopping it from being shut down. These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Emotet shutdown) Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.
Name
Application Layer Protocol
ID
T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

File and Directory Discovery

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Indicator

Name
5.252.23.116
Description
CC=SK ASN=AS61424 eServer s.r.o.
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.252.23.116']
Name
98a30c7251cf622bd4abce92ab527c3f233b817a57519c2dd2bf8e3d3ccb7db8
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'cec425b3383890b63f5022054c396f6d510fae436041add935cd6ce42033f621']

Name

ed0c3e75b7ac2587a5892ca951707b4e0dd9c8b18aaf8590c24720d73aa6b90c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ed0c3e75b7ac2587a5892ca951707b4e0dd9c8b18aaf8590c24720d73aa6b90c']

Name

209.222.103.170

Description

CC=US ASN=AS23470 RELIABLESITE

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.222.103.170']

Name

110e301d3b5019177728010202c8096824829c0b11bb0dc0bff55547ead18286

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '110e301d3b5019177728010202c8096824829c0b11bb0dc0bff55547ead18286']

Name

2ccf7e42afd3f6bf845865c74b2e01e2046e541bb633d037b05bd1cdb296fa59

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2ccf7e42afd3f6bf845865c74b2e01e2046e541bb633d037b05bd1cdb296fa59']

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
b5ef11d04604c9145e4fe1bedaeb52f2c2345703d52115a5bf11ea56d7fb6b03
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b5ef11d04604c9145e4fe1bedaeb52f2c2345703d52115a5bf11ea56d7fb6b03']
Name
58ccfb603cdc4d305fddd52b84ad3f58ff554f1af4d7ef164007cb8438976166
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '58ccfb603cdc4d305fddd52b84ad3f58ff554f1af4d7ef164007cb8438976166']

Name

a8f6c1ccba662a908ef7b0cb3cc59c2d1c9e2cbbe1866937da81c4c616e68986

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a8f6c1ccba662a908ef7b0cb3cc59c2d1c9e2cbbe1866937da81c4c616e68986']

Name

dojustit.mooo.com

Pattern Type

stix

Pattern

[hostname:value = 'dojustit.mooo.com']

Name

5.252.25.88

Description
CC=DE ASN=AS202422 G-Core Labs S.A.
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.252.25.88']
Name
1826268249e1ea58275328102a5a8d158d36b4fd312009e4a2526f0bfbc30de2
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '1826268249e1ea58275328102a5a8d158d36b4fd312009e4a2526f0bfbc30de2']
Name
148.113.152.144
Description
CC=CA ASN=AS16276 OVH SAS
Pattern Type

stix

Pattern

[ipv4-addr:value = '148.113.152.144']

Name

198.12.76.214

Description

CC=US ASN=AS36352 AS-COLOCROSSING

Pattern Type

stix

Pattern

[ipv4-addr:value = '198.12.76.214']

Name

209.97.137.33

Description

CC=GB ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.97.137.33']

Name

0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e9']

Name

84.234.96.104

Description

CC=RO ASN=AS51177 Tipzor Media Srl

Pattern Type

stix

Pattern

[ipv4-addr:value = '84.234.96.104']

Vulnerability

Name
CVE-2023-34362

StixFile

Value
ed0c3e75b7ac2587a5892ca951707b4e0dd9c8b18aaf8590c24720d73aa6b90c
a8f6c1ccba662a908ef7b0cb3cc59c2d1c9e2cbbe1866937da81c4c616e68986
2ccf7e42afd3f6bf845865c74b2e01e2046e541bb633d037b05bd1cdb296fa59
b5ef11d04604c9145e4fe1bedaeb52f2c2345703d52115a5bf11ea56d7fb6b03
cec425b3383890b63f5022054c396f6d510fae436041add935cd6ce42033f621
98a30c7251cf622bd4abce92ab527c3f233b817a57519c2dd2bf8e3d3ccb7db8
58ccfb603cdc4d305fddd52b84ad3f58ff554f1af4d7ef164007cb8438976166
110e301d3b5019177728010202c8096824829c0b11bb0dc0bff55547ead18286
1826268249e1ea58275328102a5a8d158d36b4fd312009e4a2526f0bfbc30de2
0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e9

Hostname

Value
dojustit.mooo.com

IPv4-Addr

Value
5.252.23.116
89.39.105.108
209.222.103.170
5.252.25.88
84.234.96.104
198.12.76.214
209.97.137.33
148.113.152.144

External References

- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/trustwave-action-response-zero-day-exploitation-of-moveit-cve-2023-34362/
- https://otx.alienvault.com/pulse/647efbbf9d4d077da2df7dee