Oct 05 2023

NETMANAGEIT

Intelligence Report

Threat Brief - MOVEit Transfer SQL Injection Vulnerabilities: CVE-2023-34362, CVE-2023-35036 and CVE-2023-35708

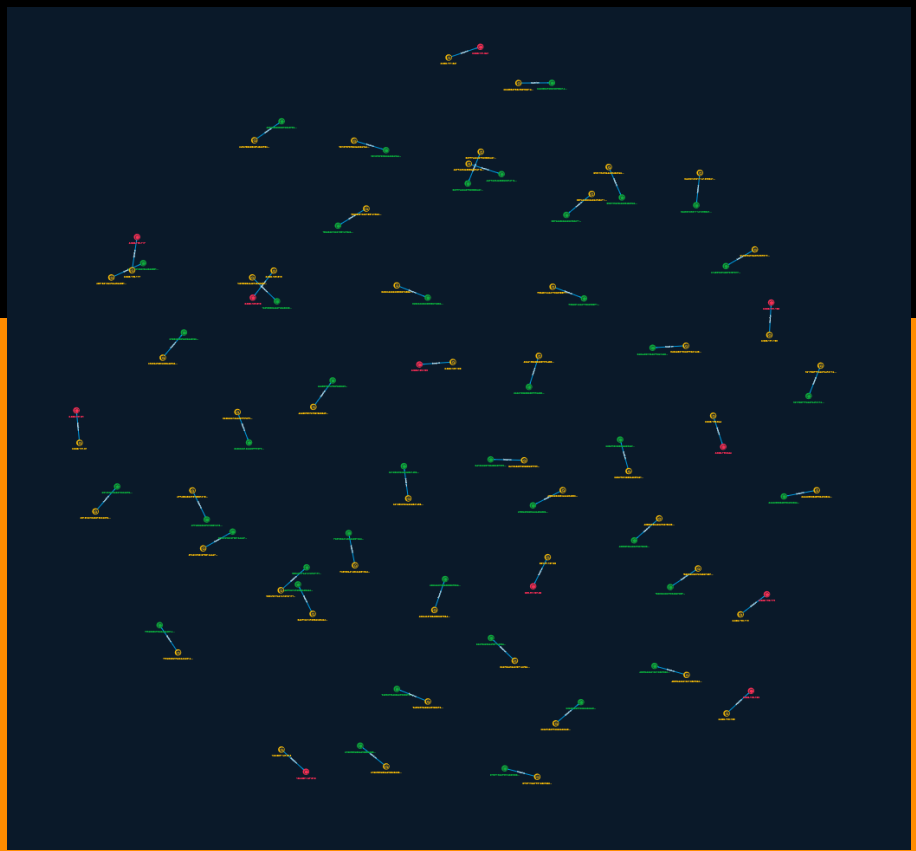

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This threat brief details the critical vulnerability CVE-2023-34362 found in MOVEit Transfer.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
3c0dbda8a5500367c22ca224919bfc87d725d890756222c8066933286f26494c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '3c0dbda8a5500367c22ca224919bfc87d725d890756222c8066933286f26494c']
Name
2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5']
Name

929bf317a41b187cf17f6958c5364f9c5352003edca78a75ee33b43894876c62

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '929bf317a41b187cf17f6958c5364f9c5352003edca78a75ee33b43894876c62']

Name

f3543cd16de13214124bd7c91033c3cd3bbcf6587871257e699fd89df96fd86f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f3543cd16de13214124bd7c91033c3cd3bbcf6587871257e699fd89df96fd86f']

Name

bdd4fa8e97e5e6eaaac8d6178f1cf4c324b9c59fc276fd6b368e811b327ccf8b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bdd4fa8e97e5e6eaaac8d6178f1cf4c324b9c59fc276fd6b368e811b327ccf8b']

Name

5b566de1aa4b2f79f579cdac6283b33e98fdc8c1cfa6211a787f8156848d67ff

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5b566de1aa4b2f79f579cdac6283b33e98fdc8c1cfa6211a787f8156848d67ff']

Name

348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d']

Name

165.227.147.215

Description

Agressive IP known malicious on AbuseIPDB - countryCode: DE - abuseConfidenceScore: 100 - lastReportedAt: 2023-10-04T15:03:44+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '165.227.147.215']

Name

702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0']

Name

9e89d9f045664996067a05610ea2b0ad4f7f502f73d84321fb07861348fdc24a

Pattern Type

stix

Pattern

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

Name

b9a0baf82feb08e42fa6ca53e9ec379e79fbe8362a7dac6150eb39c2d33d94ad

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b9a0baf82feb08e42fa6ca53e9ec379e79fbe8362a7dac6150eb39c2d33d94ad']

Name

387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a

Description

SHA256 of 44d8e68c7c4e04ed3adacb5a88450552

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a']

Name

6e1d3b5fcb4de48e1e06a68686817d13533f9740e315f4378bb5b9ef1fd1c7a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6e1d3b5fcb4de48e1e06a68686817d13533f9740e315f4378bb5b9ef1fd1c7a9']

Name

93137272f3654d56b9ce63bec2e40dd816c82fb6bad9985bed477f17999a47db

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '93137272f3654d56b9ce63bec2e40dd816c82fb6bad9985bed477f17999a47db']

Name

cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45

Description

SHA256 of b69e23cd45c8ac71652737ef44e15a34

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45']

Name

ea433739fb708f5d25c937925e499c8d2228bf245653ee89a6f3d26a5fd00b7a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea433739fb708f5d25c937925e499c8d2228bf245653ee89a6f3d26a5fd00b7a']

Name

3a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d3c2a74545725b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d3c2a74545725b']

Name

5.252.191.103

Description
CC=US ASN=AS62240 Clouvider Limited
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.252.191.103']
Name
e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e']
Name
b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272
Pattern Type
stix
Pattern

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

Name

24c7fae1b7c02ebd84cc3c78553fb3a68d0466575abea4c92b2f792b47c41ef3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '24c7fae1b7c02ebd84cc3c78553fb3a68d0466575abea4c92b2f792b47c41ef3']

Name

d477ec94e522b8d741f46b2c00291da05c72d21c359244ccb1c211c12b635899

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd477ec94e522b8d741f46b2c00291da05c72d21c359244ccb1c211c12b635899']

Name

f0d85b65b9f6942c75271209138ab24a73da29a06bc6cc4faeddcb825058c09d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f0d85b65b9f6942c75271209138ab24a73da29a06bc6cc4faeddcb825058c09d']

Name

5.252.190.117

Description

CC=US ASN=AS62240 Clouvider Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.252.190.117']

Name

daaa102d82550f97642887514093c98ccd51735e025995c2cc14718330a856f4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'daaa102d82550f97642887514093c98ccd51735e025995c2cc14718330a856f4']

Name
5.252.190.100
Description
CC=US ASN=AS62240 Clouvider Limited
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.252.190.100']
Name
d49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195']
Name
c82059564d6e7a6f56d3b1597cdfe98dfc4e30a2050024bd744f12a3ef237bb5
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c82059564d6e7a6f56d3b1597cdfe98dfc4e30a2050024bd744f12a3ef237bb5']

Name

7a8f53c4143bacd2104ccd07a6be68d76cda1a6985b8573b7735858a542178bb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7a8f53c4143bacd2104ccd07a6be68d76cda1a6985b8573b7735858a542178bb']

Name

2931994f3bde59c3d9da53e0062e4d993dc6fc655a1bd325e90af6dc494ed1fa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2931994f3bde59c3d9da53e0062e4d993dc6fc655a1bd325e90af6dc494ed1fa']

Name

4359aead416b1b2df8ad9e53c497806403a2253b7e13c03317fc08ad3b0b95bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4359aead416b1b2df8ad9e53c497806403a2253b7e13c03317fc08ad3b0b95bf']

Name

87ebfaf36fc7031bec477c70a86cb746811264f530d8af419767b9755e2b43e3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '87ebfaf36fc7031bec477c70a86cb746811264f530d8af419767b9755e2b43e3']

Name

9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a1269294254e958e0e58fc0fe887ebbc4201d5c266557f09c3f37542bd6d53d7']

Name

fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f

Description

SHA256 of a85299f78ab5dd05e7f0f11ecea165ea

Pattern Type

stix

Pattern

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

Name

de4ad0052c273649e0aca573e30c55576f5c1de7d144d1d27b5d4808b99619cd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de4ad0052c273649e0aca573e30c55576f5c1de7d144d1d27b5d4808b99619cd']

Name

5.252.191.31

Description

CC=US ASN=AS62240 Clouvider Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.252.191.31']

Name

0ea05169d111415903a1098110c34cdbbd390c23016cd4e179dd9ef507104495

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0ea05169d111415903a1098110c34cdbbd390c23016cd4e179dd9ef507104495']

Name

3ff0719da7991a38f508e72e32412a1ee498241bf84f65e973d6e93dc8fd1f66

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3ff0719da7991a38f508e72e32412a1ee498241bf84f65e973d6e93dc8fd1f66']

Name

c77438e8657518221613fbce451c664a75f05beea2184a3ae67f30ea71d34f37

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c77438e8657518221613fbce451c664a75f05beea2184a3ae67f30ea71d34f37']

Name

209.97.137.33

Description

CC=GB ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.97.137.33']

Name

c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4

Pattern Type

stix

Pattern

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

Name

bd45234763ef62f05d14b78c6497ed90706a271fad3b16a4ee6d99d178beedf3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd45234763ef62f05d14b78c6497ed90706a271fad3b16a4ee6d99d178beedf3']

Name

ba2cf96fc5884cd69ecfe5d73f872958159a12b02ca610223f089ee0b6c3d25d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ba2cf96fc5884cd69ecfe5d73f872958159a12b02ca610223f089ee0b6c3d25d']

Name

6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d

Pattern Type

stix

Pattern

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

Name

5.252.190.244

Description

CC=US ASN=AS62240 Clouvider Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.252.190.244']

Name

5.252.190.119

Description

CC=US ASN=AS62240 Clouvider Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.252.190.119']

Name

5.252.191.241

Description

CC=US ASN=AS62240 Clouvider Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.252.191.241']

Name

5.252.189.130

Description

CC=US ASN=AS62240 Clouvider Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.252.189.130']

Name

f994063b9fea6e4b401ee542f6b6d8d6d3b9e5082b5313adbd02c55dc6b4feb7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f994063b9fea6e4b401ee542f6b6d8d6d3b9e5082b5313adbd02c55dc6b4feb7']

Name
5.252.189.210
Description
CC=US ASN=AS62240 Clouvider Limited
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.252.189.210']
Name
3ab73ea9aebf271e5f3ed701286701d0be688bf7ad4fb276cb4fbe35c8af8409
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '3ab73ea9aebf271e5f3ed701286701d0be688bf7ad4fb276cb4fbe35c8af8409']

StixFile

Value
929bf317a41b187cf17f6958c5364f9c5352003edca78a75ee33b43894876c62
f0d85b65b9f6942c75271209138ab24a73da29a06bc6cc4faeddcb825058c09d
3a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d3c2a74545725b
3c0dbda8a5500367c22ca224919bfc87d725d890756222c8066933286f26494c
2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5
348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d
3ff0719da7991a38f508e72e32412a1ee498241bf84f65e973d6e93dc8fd1f66
24c7fae1b7c02ebd84cc3c78553fb3a68d0466575abea4c92b2f792b47c41ef3
de4ad0052c273649e0aca573e30c55576f5c1de7d144d1d27b5d4808b99619cd
f994063b9fea6e4b401ee542f6b6d8d6d3b9e5082b5313adbd02c55dc6b4feb7
7a8f53c4143bacd2104ccd07a6be68d76cda1a6985b8573b7735858a542178bb
87ebfaf36fc7031bec477c70a86cb746811264f530d8af419767b9755e2b43e3
ba2cf96fc5884cd69ecfe5d73f872958159a12b02ca610223f089ee0b6c3d25d

b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272

fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f

387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a

4359aead416b1b2df8ad9e53c497806403a2253b7e13c03317fc08ad3b0b95bf

3ab73ea9aebf271e5f3ed701286701d0be688bf7ad4fb276cb4fbe35c8af8409

c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4

5b566de1aa4b2f79f579cdac6283b33e98fdc8c1cfa6211a787f8156848d67ff

b9a0baf82feb08e42fa6ca53e9ec379e79fbe8362a7dac6150eb39c2d33d94ad

2931994f3bde59c3d9da53e0062e4d993dc6fc655a1bd325e90af6dc494ed1fa

cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45

ea433739fb708f5d25c937925e499c8d2228bf245653ee89a6f3d26a5fd00b7a

bdd4fa8e97e5e6eaaac8d6178f1cf4c324b9c59fc276fd6b368e811b327ccf8b

f3543cd16de13214124bd7c91033c3cd3bbcf6587871257e699fd89df96fd86f

d477ec94e522b8d741f46b2c00291da05c72d21c359244ccb1c211c12b635899

a1269294254e958e0e58fc0fe887ebbc4201d5c266557f09c3f37542bd6d53d7

6e1d3b5fcb4de48e1e06a68686817d13533f9740e315f4378bb5b9ef1fd1c7a9

702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0

9e89d9f045664996067a05610ea2b0ad4f7f502f73d84321fb07861348fdc24a

93137272f3654d56b9ce63bec2e40dd816c82fb6bad9985bed477f17999a47db

c77438e8657518221613fbce451c664a75f05beea2184a3ae67f30ea71d34f37

e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e

0ea05169d111415903a1098110c34cdbbd390c23016cd4e179dd9ef507104495

c82059564d6e7a6f56d3b1597cdfe98dfc4e30a2050024bd744f12a3ef237bb5

d49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195

9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead

6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d

bd45234763ef62f05d14b78c6497ed90706a271fad3b16a4ee6d99d178beedf3

daaa102d82550f97642887514093c98ccd51735e025995c2cc14718330a856f4

IPv4-Addr

Value
5.252.189.130
5.252.191.241
165.227.147.215
5.252.190.117
5.252.190.100
5.252.189.210
5.252.191.103
5.252.190.244
5.252.191.31
5.252.190.119
209.97.137.33

External References

- https://otx.alienvault.com/pulse/651e87d9ab960ad52a24ad67
- https://unit42.paloaltonetworks.com/threat-brief-moveit-cve-2023-34362/#post-128425-_ydqdbjg0dngh