America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBERSECURITY ADVISORY

Threat Actors Exploiting Ivanti EPMM Vulnerabilities

Release Date: August 01, 2023 **Alert Code:** AA23-213A

RELATED TOPICS: SECURING NETWORKS </topics/cyber-threats-and-advisories/securing-networks>, CYBER THREATS AND ADVISORIES </topics/cyber-threats-and-advisories>

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) and the Norwegian National Cyber Security Centre (NCSC-NO) are releasing this joint Cybersecurity Advisory (CSA) in response to active exploitation of CVE-2023-35078 and CVE-2023-35081. Advanced persistent threat (APT) actors exploited CVE-2023-35078 as a zero day from at least April 2023 through July 2023 to gather information from several Norwegian organizations, as well as to gain access to and compromise a Norwegian government agency's network.

Ivanti released a patch for CVE-2023-35078 on July 23, 2023. Ivanti later determined actors could use CVE-2023-35078 in conjunction with another vulnerability CVE-2023-35081 and released a patch for the second vulnerability on July 28, 2023. NCSC-NO observed possible vulnerability chaining of CVE-2023-35081 and CVE-2023-35078.

CVE-2023-35078 is a critical vulnerability affecting Ivanti Endpoint Manager Mobile (EPMM) (formerly known as MobileIron Core). The vulnerability allows threat actors to access personally identifiable information (PII) and gain the ability to make configuration changes on compromised systems. CVE-2023-35081 enables actors with EPMM administrator privileges to write arbitrary files with the operating system privileges of the EPMM web application server. Threat actors can chain these vulnerabilities to gain initial, privileged access to EPMM systems and execute uploaded files, such as webshells.

Mobile device management (MDM) systems are attractive targets for threat actors because they provide elevated access to thousands of mobile devices, and APT actors have exploited a previous MobileIron vulnerability. Consequently, CISA and NCSC-NO are concerned about the potential for widespread exploitation in government and private sector networks.

This CSA provides indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) obtained by NCSC-NO investigations. The CSA also includes a nuclei template to identify unpatched devices and detection guidance organizations can use to hunt for compromise. CISA and NCSC-NO encourage organizations to hunt for malicious activity using the detection guidance in this CSA. If potential compromise is detected, organizations should apply the incident response recommendations included in this CSA. If no compromise is detected, organizations should still immediately apply patches released by Ivanti.

Download the PDF version of this report:

AA23-213A PDF </sites/default/files/2023-08/aa23-213a_joint_csa_threat_actors_exploiting_ivanti_eppm_vulnerabilities_1.pdf>
(PDF, 492.43 KB)

Download the .xml or .json file associated with this report:

AA23-213A STIX XML </sites/default/files/2023-08/aa23-213a.stix_.xml>

(XML, 277.43 KB)

AA23-213A STIX JSON </sites/default/files/2023-08/aa23-213a%20threat%20actors%20exploiting%20ivanti%20epmm%20vulnerabilities.stix_.json>

(JSON, 250.01 KB)

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise <https://attack.mitre.org/versions/v13/matrices/enterprise/> framework, version 13. See the MITRE ATT&CK Tactics and Techniques section of this advisory for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping <https://www.cisa.gov/news-events/news/best-practices-mitre-attckr-mapping> and CISA's Decider Tool <https://github.com/cisagov/decider/>.

Overview

In July 2023, NCSC-NO became aware of APT actors exploiting a zero-day vulnerability in Ivanti Endpoint Manager (EPMM), formerly known as MobileIron Core, to target a Norwegi government network. Ivanti confirmed that the threat actors exploited CVE-2023-35078 ar released a patch on July 23, 2023.[1] Ivanti later determined actors could use CVE-2023-35078 in conjunction with another vulnerability, CVE-2023-35081, and released a patch for the second vulnerability on July 28, 2023.[2]

CVE-2023-35078 <https://nvd.nist.gov/vuln/detail/cve-2023-35078> is a critical authentication bypass [CWE-288] <https://cwe.mitre.org/data/definitions/288.html> vulnerability affecting Ivanti Endpoint Manager Mobile (EPMM), formerly known as MobileIron Core. The vulnerability allows unauthenticated access to specific application programming interface (API) paths. Threat actors with access to these API paths can access PII such as names, phone numbers,

and other mobile device details of users on the vulnerable system; make configuration changes to vulnerable systems; push new packages to mobile endpoints; and access Global Positioning System (GPS) data if enabled.

According to Ivanti, CVE-2023-35078 can be chained with a second vulnerability CVE-2023-35081 <https://nvd.nist.gov/vuln/detail/cve-2023-35081>.[2] CVE-2023-35081 is directory traversal vulnerability [CWE-22 <https://cwe.mitre.org/data/definitions/22.html>] in EPMM. This vulnerability allows threat actors with EPMM administrator privileges the capability to write arbitrary files, such as webshells, with operating system privileges of the EPMM web application server. The actors can then execute the uploaded file.[2]

CISA added CVE-2023-35078 to its Known Exploited Vulnerabilities Catalog <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> on July 25, 2023, and CVE-2023-35081 on July 31, 2023.

CISA and NCSC-NO are concerned about the potential for widespread exploitation of both vulnerabilities in government and private sector networks because MDM systems provide elevated access to thousands of mobile devices. Threat actors, including APT actors, have previously exploited a MobileIron vulnerability [3 <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-275a>],[4 <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-209a>].

APT Actor Activity

The APT actors have exploited CVE-2023-35078 since at least April 2023. The actors leveraged compromised small office/home office (SOHO) routers, including ASUS routers, to proxy [T1090 <https://attack.mitre.org/versions/v13/techniques/t1090/>] to target infrastructure, and NCSC-NO observed the actors exploiting CVE-2023-35078 to obtain initial access to EPMM devices [T1190 <https://attack.mitre.org/versions/v13/techniques/t1190/>] and:

- Perform arbitrary Lightweight Directory Access Protocol (LDAP) queries against the Active Directory (AD).
- Retrieve LDAP endpoints [T1018 <https://attack.mitre.org/versions/v13/techniques/t1018/>].

- Use API path `/mifs/aad/api/v2/authorized/users` to list users and administrators [T1087.002 <https://attack.mitre.org/versions/v13/techniques/t1087/002/>] on the EPMM device.
- Make EPMM configuration changes (**Note:** It is unknown what configuration changes the actors made).
- Regularly check EPMM Core audit logs [T1005 <https://attack.mitre.org/versions/v13/techniques/t1005>].

The APT actors deleted some of their entries in Apache httpd logs [T1070 <https://attack.mitre.org/versions/v13/techniques/t1070/001/>] using `mi.war`, a malicious Tomcat application that deletes log entries based on the string in `keywords.txt`. The actors deleted log entries with the string `Firefox/107.0`.

The APT actors used Linux and Windows user agents with `Firefox/107.0` to communicate with EPMM. Other agents were used; however, these user agents did not appear in the device logs. It is unconfirmed how the threat actors ran shell commands on the EPMM device; however, NCSC-NO suspects the actors exploited CVE-2023-35081 to upload webshells on the EPMM device and run commands [T1059 <https://attack.mitre.org/versions/v13/techniques/t1059/>].

The APT actors tunneled traffic [T1572 <https://attack.mitre.org/versions/v13/techniques/t1572/>] from the internet through Ivanti Sentry, an application gateway appliance that supports EPMM, to at least one Exchange server that was not accessible from the internet [T1090.001 <https://attack.mitre.org/versions/v13/techniques/t1090/001/>]. It is unknown how they tunneled traffic. NCSC-NO observed that the network traffic used the TLS certificate of the internal Exchange server. The APT actors likely installed webshells [T1505.003 <https://attack.mitre.org/versions/v13/techniques/t1505/003/>] on the Exchange server in the following paths [T1036.005 <https://attack.mitre.org/versions/v13/techniques/t1036/005/>]:

- `/owa/auth/logon.aspx`
- `/owa/auth/logoff.aspx`
- `/owa/auth/OutlookCN.aspx`

NCSC-NO also observed `mi.war` on Ivanti Sentry but do not know how the actors placed it there.

MITRE ATT&CK TACTICS AND TECHNIQUES

See Table 1—Table 7 for all referenced threat actor tactics and techniques in this advisory.

Table 1: APT Actors ATT&CK Techniques for Initial Access

Technique Title	ID	Use
Exploit Public-Facing Application	T1190 <https://attack.mitre.org/versions/v13/techniques/t1190/>	The APT actors exploited CVE-2023-35078 in public facing Ivanti EPMM appliances since at least April 2023.

Table 2: APT Actors ATT&CK Techniques for Execution

Technique Title	ID	Use
Command and Scripting Interpreter	T1059 <https://attack.mitre.org/versions/v13/techniques/t1059/>	The APT actors may have exploited CVE-2023-35081 to upload webshells on the EPMM device and run commands.

Table 3: APT Actors ATT&CK Techniques for Discovery

Technique Title	ID	Use
Account Discovery: Domain Account	T1087.002 <https://attack.mitre.org/versions/v13/techniques/t1087/002/>	The APT actors exploited CVE-2023-35078 to gather EPMM device users and administrators.
Remote System Discovery	T1018 <https://attack.mitre.org/versions/v13/techniques/t1018/>	The APT actors retrieved LDAP endpoints.

Table 4: APT Actors ATT&CK Techniques for Persistence

Technique Title	ID	Use
Masquerading: Match Legitimate Name or Location	T1036.005 <https://attack.mitre.org/versions/v13/techniques/t1036/005/>	The APT actors likely installed webshells at legitimate Exchange server paths.
Server Software Component: Web Shell	T1505.003 <https://attack.mitre.org/versions/v13/techniques/t1505/003/>	The APT actors implanted webshells on the compromised infrastructure.

Table 5: APT Actor ATT&CK Techniques for Defense Evasion

Technique Title	ID	Use
Indicator Removal	T1070 <https://attack.mitre.org/versions/v13/techniques/t1070/001/>	APT actors deleted httpd access logs after the malicious activities took place using string `Firefox/107.0`.

Table 6: APT Actor ATT&CK Techniques for Collection

Technique Title	ID	Use
Data from Local System	T1005 <https://attack.mitre.org/versions/v13/techniques/t1005/>	APT actors regularly checked EPMM Core audit logs.

Table 7: APT Actor ATT&CK Techniques for Command and Control

Technique Title	ID	Use
Protocol Tunneling	T1572 <https://attack.mitre.org/versions/v13/techniques/t1572/>	The APT actors tunneled traffic from the internet to an Exchange server that was not accessible from the internet.

Technique Title	ID	Use
Proxy	T1090 <https://attack.mitre.org/versions/v13/techniques/t1090/>	The actors leveraged compromised SOHO routers to proxy to and compromise infrastructure. The actors tunneled traffic from the internet to at least one Exchange server.
Proxy: Internal Proxy	T1090.001 <https://attack.mitre.org/versions/v13/techniques/t1090/001/>	The APT actors tunneled traffic from the internet to an Exchange server that was not accessible from the internet.

EVIDENCE OF VULNERABILITY METHODS

CISA recommends administrators use the following CISA-developed nuclei template to determine vulnerability to CVE-2023-30578:

```
id: CVE-2023-35078-Exposure

info:
  name: Ivanti EPMM Remote Unauthenticated API Access
  author: JC
  severity: critical
  reference:
    - https://nvd.nist.gov/vuln/detail/CVE-2023-35078
```
<https://nvd.nist.gov/vuln/detail/cve-2023-35078>
```
  description: Identifies vulnerable instances of Ivanti Endpoint Manager Mobile (EPMM), formerly MobileIron Core, through 11.10 allows remote attackers to obtain PII, add an administrative account, and change the configuration because of an authentication bypass.
  tags: ivanti, mobileiron, epmm, auth-bypass

requests:
  - method: GET
    path:
      - "{{RootURL}}/mifs/aad/api/v2/ping"

    matchers-condition: and
    matchers:
```

```
      - type: status
        status:
          - 200

      - type: word
        part: body
        words:
          - "vspVersion"
          - "apiVersion"
        condition: and
```

CISA recommends administrators use the following CISA-developed nuclei template to determine vulnerability to CVE-2023-35081:

```
id: CVE-2023-35081

info:
  name: Ivanti EPMM Remote Arbitrary File Write
  author: JC
  severity: High
  reference:
    - https://nvd.nist.gov/vuln/detail/CVE-2023-35081
```
<https://nvd.nist.gov/vuln/detail/cve-2023-35081>
```
  description: Identifies vulnerable unpatched versions of Ivanti Endpoint Manager Mobile (EPMM), formerly MobileIron Core, through 11.10.0.3, 11.9.1.2, and 11.8.1.2 that allows an authenticated administrator to perform arbitrary file writes to the EPMM server.
  tags: ivanti, mobileiron, epmm

requests:
  - method: GET
    path:
      - "{{RootURL}}/mifs/c/windows/api/v2/device/registration"

    matchers-condition: and
    matchers:
```

```
      - type: status
        status:
          - 200

      - type: regex
        part: all
        regex:
          - '.*\?VSP ((0?[0-9]|10)(\.\d+){1,3}|11\.(0?[0-7])
(\.\d+){1,2}|11\.8\.0(\.\d+)?|11\.8\.1\.[0-1]|11\.9\.0(\.\d+)?
|11\.9\.1\.[0-1]|11\.10\.0\.[0-2]).*'
```

Run the following NCSC-NO-created checks to check for signs of compromise:

1. Investigate logs in centralized logging solutions or forwarded `syslogs` from EPMM devices for any occurrences of `/mifs/aad/api/v2/`.
2. Look for spikes or an increase of `EventCode=1644` in the AD since at least April 202 The LDAP queries performed by EPMM when the threat actor used the MIFS API generated tens of millions of this event code. Also look for EventCodes `4662`, `5136`, and `1153`.
3. To detect tunneling activity through Sentry, look for traffic from EPMM devices to other internal servers, as well as TLS traffic towards instances of EPMM with different TLS certificates than the instance itself would possess. Traffic to EPMM with certificates originating from endpoints further inside the network, e.g. standard Windows generated certificates such as `CN=EXCHANGE01` or similar.
4. Perform forensic analysis of disk and memory since log retention may be poor and threat actors have been observed deleting log entries. Pay particular attention to unallocated disk space (free space on filesystem).

5. Check for activity from ASUS routers in your own country towards EPMM and Sentry devices.

INCIDENT RESPONSE

If compromise is detected, organizations should:

1. Quarantine or take offline potentially affected hosts.
2. Reimage compromised hosts.
3. Provision new account credentials.
4. Collect and review artifacts such as running processes/services, unusual authentications, and recent network connections.
5. Report the compromise to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 1-844-Say-CISA) or to NCSC-NO via NCSC-NO's 24/7 Operations Center (cert@ncsc.no or +47 23 31 07 50).

MITIGATIONS

CISA and NCSC-NO recommend organizations:

- **Upgrade Ivanti EPMM versions to the latest version** as soon as possible. See Ivanti CVE-2023-35081 - Remote Arbitrary File Write for patch information. This patch protects against CVE-2023-35078 and CVE-2023-35081.
  - See the Evidence of Vulnerability Methods section of this advisory for CISA-developed nuclei templates to find any EPMM versions vulnerable to CVE-2023-35078 and CVE-2023-35081.
  - Organizations using unsupported versions (i.e., versions prior to 11.8.1.0) should immediately upgrade to a supported version. If you cannot immediately upgrade, apply the Ivanti-provided RPM fix for CVE-35078 (this workaround does not protect against CVE-2023-35081):
    - Login to command line shell (CLI) in enable mode.
    - Run the following command: `# install rpm url https://support.mobileiron.com/ivanti-updates/ivanti-security-update-1.0.0-1.noarch.rp`
    - See Ivanti's Knowledge Base (KB) Remote unauthenticated API access vulnerability - CVE-2023-35078 for more information on the RPM fix.
- **Treat MDM systems as high-value assets (HVAs) with additional restrictions and monitoring**. MDM systems provide elevated access to thousands of hosts and should be treated as high value assets (HVAs) with additional restrictions and monitoring.
- **Follow best cybersecurity practices** in production and enterprise environments, including mandating phishing-resistant multifactor authentication (MFA) <https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf> for all staff and services. For additional best practices, see CISA's Cross-Sector Cybersecurity Performance Goals <https://www.cisa.gov/cpg> (CPGs). The CPGs, developed by CISA and the National Institute of Standards and Technology (NIST), are a prioritized subset of IT and OT security practices that can meaningfully reduce the likelihood and impact of known cyber risks and common TTPs. Because the CPGs are a subset of best practices, CISA and NCSC-NO also recommend software manufacturers implement a comprehensive information security program based on a recognized framework, such as the NIST Cybersecurity Framework (CSF).

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA and NCSC-NO recommends exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise <https://attack.mitre.org/versions/v13/matrices/enterprise/> framework in this advisory. CISA recommends testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Table 1–Table 7).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA recommends continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

Give Feedback

REFERENCES

[1] Ivanti: CVE-2023-35078 – Remote Unauthenticated API Access Vulnerability

[2] Ivanti: CVE-2023-35081 – Remote Arbitrary File Write

[3] CISA: Potential for China Cyber Response to Heightened U.S.-China Tensions <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-275a>

[4] CISA: Top Routinely Exploited Vulnerabilities <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-209a>

RESOURCES

- Mnemonic: Ivanti Endpoint Manager Mobile (EPMM) Authentication Bypass Vulnerability <https://www.mnemonic.io/resources/blog/ivanti-endpoint-manager-mobile-epmm-authentication-bypass-vulnerability/>
- Mnemonic: Threat Advisory: Remote File Write Vulnerability in Ivanti EPMM <https://www.mnemonic.io/resources/blog/threat-advisory-remote-file-write-vulnerability-in-ivanti-epmm/>

ACKNOWLEDGEMENTS

Ivanti contributed to this joint advisory.

NCSC-NO wishes to acknowledge Mnemonic's contributions.

VERSION HISTORY

August 1, 2023: Initial version.

August 2, 2023: Added stix file, updated Acknowledgements section, and added Resources section.

APPENDIX: INDICATORS OF COMPROMISE

NCSC-NO observed the following webshell hash:

```
c0b42bbd06d6e25dfe8faebd735944714b421388
```

NCSC-NO observed the following hash of `mi.war`:

```
1cd358d28b626b7a23b9fd4944e29077c265db46
```

NCSC-NO observed the following JA3 hashes used against MobileIron Core:

2d5bd942ebf308df61e1572861d146f6

473cd7cb9faa642487833865d516e578

579ccef312d18482fc42e2b822ca2430

849d3331f3e07a0797a02f12a6a82aa9

8d9f7747675e24454cd9b7ed35c58707

ad55557b7cbd735c2627f7ebb3b3d493

cd08e31494f9531f560d64c695473da9

e1d8b04eeb8ef3954ec4f49267a783ef

e60dc8370ecf78cf115162fbc257baf5

e669667efb41c36f714c309243f41ca7

e84a32d43db750b206cb6beed08281d0

eb5fdc72f0a76657dc6ea233190c4e1c

NCSC-NO observed the following JA3 hashes used against Exchange when tunneling via EPMM Sentry:

0092ce298a1d451fbe93dc4237053a96

00e872019b976e69a874ee7433038754

01ecd9ab9be75e832c83c082be3bdf18

0212a88c7ed149febdefa347c610b248

02be3b93640437dbba47cc7ed5ab7895

03f8852448a85e14f2b4362194160c32

045f8ccdac6d4e769b30da406808da71

04e7f5787f89a597001b50a37b9f8078

070f9fe9f0ec69e6b8791d280fde6a48

07a624d7236cca3934cf1f8e44b74b52

09df72c01a1a0ad193e2fff8e454c9c4

0b28842d64a344c287e6165647f3b3fe

0b8e1211de50d244b89e6c1b366d3ccf

0cb0380cf75a863b3e40a0955b1ada9f

0da24834056873a8cd8311000088e8be

0e1fad8ffaa7a939f0a6cbf9cd7e2fcd

0f6e78839398c245d13f696a3216d840

119f8c9050d1499b6f958b857868b8ce

11c506d5e3fb7e119c4287202c96a930

1336df27f94b25a25acac9db3e61e461

14671c3f8deca7d73a03b74cb854c21d

146caf9bd0153428f54e9ef472154983

14994353f3ea6fd25952a8c7d57f9ecf

151bc875df15d1385e6eb02f9edaba06

15a074a397727b26a846b443b99c20ff

1660f3d882a4311ca013ee4586e01fd9

16a74fc216f8a4ce43466bb83b6d3fd2

188623fdd056c4ed13d1ff34c7377637

19f51486abd40c9f0fc0503559a6c523

1a024e63721c610d2e54e67d62cd5460

1aa7dae8f2ae0a29402ed51819f82db4

1abfdeaadb74a0f7c461e7bab157b17f

1b6720ed0b67c910a80722ce973d6217

1b7d9368c6ce7623fdbc43f013626535

1e0850e10a00c9bbdd5c582ff4cb6833

1ec71612e438cf902913eec993475eb9

206fed3a39d9215c35395663f5bb3307

22cc1b3bc9f99d3a520ae58fee79a0d5

23e3e6fa8b23d9bc19e82de4e64c79e9

253fd4659bf21be116858bc0f206c5b9

276e175d4fe8454c4c47e966d8cb3fa3

289a450c7478dd52a10c6ed2fb47f7e9

2aa8ba7478b1362274666d714df575bc

2beecb6b9e386f29d568229a9953c3d2

2ebc7fdceaa9a0df556e989d77157006

3003024afe64b4e8a5a30825c14bbb12

3082e669dda9d023e2dcd8b9549a84a8

309d33c6f77a3fc75654c44c61596ccd

30a9f568eb3df79352fc587a078623b6

30be84e6b95f44c203f8e7fce7339a8e

3268a5097a543c7dbd82c39a9193b7fe

32775ead3ea1ad7db2f4bea67fe0cabb

34ac9a6ef5d285119abec50fbe41fcfe

34d92552e278710c1e84f0bd8dc3a6b8

361f47a6357cc6e3a9bcdd20cfaaf0e9

3685abc75517e61e47e52e5f2d060f54

3744004013135b9f9a05cb58cda8134d

37d952966ea7e79277803f13d7147544

391a4c2c7541b8b78e2f99bf586e9794

393662e5aa0cb49c5d666a6d10a1ade6

3962b622c5aa815afb803b92aa948424

3b22af324abded2781ed8f6a61f3654f

3b30b4555cc8b4b164ad03cf322cbea8

3bd1bdb5e90b9590a8878bff2ada8204

3be529eb3a7daaf34f963a22188f6139

3dd13faad1c45eb0c23e4567210f7eac

403273b51f91cf3c333695e5532cb2c3

404f56045e436d53ead2177bf957ba39

41854adbc73b0b58e5c566f60bb0df25

43c22dabb1e6d2449a39c2f7e974d537

476e72bbda5b78d188766139889e3038

4898a51256ae7d914a5ffd5695973470

49230c486f0fd383cd301fe162d6a786

4959a611b9885022d81b4bc8e4b1d149

495c6ff7ca0379ad0891bac47917d09a

49d2bd08038dc7dada221008591940f9

4c1b73ec52e6eec0c5d20577fcbc9ef1

4d34db639ba84b11822fb3dac47ed7d1

5244b163f9326a1e5eaa8860f7543f99

539f1a5183800a96228458932f9307f7

5466368d4659f1b1470bcb09e65b484d

549cde6535a884126755fc53f59a820c

555389e92c622b87d3fc395fd8723501

588d0b42e54174a98e1eca59945e8b32

58bc21d305a65c41745327f142f3ac12

59401c9a60449c742d073d93d1b7039a

59eec218522cc5c7743a0d37892a3345

59faf75430e9326d3ae9d231bb3ae8c6

5d0259ca16cfc2d7d1b0fac69f29ab05

5d55026fb84dba91ac01e2095504b1bc

5e35f50c692081fd6c7ddac1272e2d6c

5f4d5965af741bba59b7c8d3425f33dd

6010282004917ecf3900babf61456432

6088c2a04c94cdcd5a283a6d1622ffba

61dee38d2f97220efb1218ad8971e3ab

62ac194f2526eb45485526bca35c8f43

634296a023280d020674c873d0199760

635755dadfab8b92fb502aafb09122db

63fc58be0d7b48eaa34da7f752ae8ae6

6441640409815cfb4bf469e685e1bdb5

646973d1928c401ba80961c12cbf84a2

65eef0a0ee257254ef0418aa57192cfb

66f6a192083a7ab00ae8e0b5cc52e8f4

67a42e2e27ffc26d1f3d0ceb8384afd0

689385f1218e0d4c347595648ca6a776

692f91c0c5e9e93e0a24bd3392887ca1

69ecf52960c8bd9e746dfe9ee19c11f6

6e359f3bbc622e9b1ed36f6e3d521bcf

6e3650528f719fc50988a1f697644832

6ead0d5d3f87911c27f3ae0a75e6b5bc

6f1fa8b444caf0d8238f948279ca74e1

6fb8cdf567dd7d89d53b5771d769cb5f

706b6055658aff067ae370f23831ef6b

708140c311d3d69418f75c928e7535a0

719ec5da8f2153a436ee8567ff609894

7292ef4cdca529071fad97496e1c9439

74871691eac48156ce0da2cfa3ab401a

74cf24f2a66a31c88b6fcfe01f12160c

75e874d8e0a79697633b87ea5e798b1c

76c0d09fed2f33babb0de8ee2c07144c

77a01363fa2b29af25c004da9570e23c

78988c65e9b70e7929e747408d8f0b0e

79c6d12d168b85437384b20eb94e106b

7b4137b4e85f31a81bb5bafeda993947

7b9db1d58326c1fa276ba2a39bcc2617

7cbc7459db5327c26476549f225030f5

7cd727171c2522f51417edeeba4f1791

7e3630c67c802eabb67b108ad4d7ded7

802f5d34c230da40c0912a1c5a9b702b

80bd0f3610f6c4d60584a5be0b8a3016

819030799f0020ed724c2ef3ffaa56c6

8207129585da68066ed08e94216d76ee

821f649d08687e22f96cea99fbb5d3a3

830838cb0620d659405a74401cd72557

833d3201066f5184c874c73a2083c448

840f488b7c0a5d686d1e89908735f354

84301b967a4d9a242466c04901bad691

85c3fac6a9885362c448f434671e362f

883b9fe16e45c388968defc73a5fba7a

8a6b0ba3496eeca39d6d3f9bae830c90

8ad0fd4b78c89bd63b97343fda1eeccb

8b0ae9029974091df12210255aaecad6

8b297f8b219e968932293ee7a8242ca3

8bb1781e756a53cd00d9b2ec670fa21e

8d5515351afdf27b013f96a05bf45147

8fafa73e9985e05d0c1c964da770c567

905967b08bd44cfa60d969229921ac23

9188ef45ea917a91ec9b92b5dd8cd90d

918dfab0333ae15d61f14fd24b5eaaac

922a3272aad17c9eaad733696a4321da

9253399537fad8448f1d4732dd79f6fa

934a8a6528e91caa019acb76e791a71d

95588e0386206fa02912cfcaf18c1220

9610328cdaa4694800c2c93410f8ce82

9622902cc43f4a20d0d686a37e4d8232

96c41e4c4a1812187fb279b9299ad63b

984c4653a563b19c87f264611a6adc01

9980febfaf901d4113a1c473f79d7eb6

9a176d818edff838fc057cea3ee372c0

9ba21c5148913186a5bf877078cbc048

9cfda02ef7e04c469b77f8197a249c17

9d74d395bd2f72a47a5c980e6040df5a

9df128ebe0c82064aa746647883112c9

9e5613533972a9d42d2e3344a4e58566

9ec17429eed5446e3720796ab50d8c60

9f2438aaab4744c4b7b5b7287a783099

9f3bf94572344b36f6ef1689cb30c66e

9fdd7a85b3a4ef8ded73beb3e6218109

a1b732a9af792f75a68ed78d72ffb8f6

a260d836428cdb971bdf147ca6940160

a4f11b1eb659869a0ae70898a4a0e5ee

a596ebbcf438980c880d711315e4fdf1

a80b6a354b493264f37aa39d0d41b5fc

a89df6156eb5a2de196388d4a123b470

a96837fe533247abb7f88000d0216a50

a98cf0a359f430a00f4f3d522f5b6cc0

aa2fe3a253e169b05e1782ca57a688d2

aef0172a2c03f77912de0bbf14aee00f

af06c3e72f2f307515ba549174d8e5a6

b311ab82b30f41b12cb9089d00c4a1ff

b4f31423445b5f13675f205ac997f41f

b50666c9aed1c2f222c56b6e9b326d27

b53f179b3f25f72bb0c7ccf45bf8beee

b57f3e41c03803306b0ee2111f7ef823

b79434613820faf30d58f103c4415a29

b8366aaa5ed51c0dea3fc90ef7e14889

b8f6b0d234a305c25411e83fd430c624

b956ed2b848dabb4e79ab7358233861b

b9ecb08402df0f1f6e1ce76b8ad6e91f

ba4a616c8d4ab9358a82b321d8e618bf

bcd62f3e029f96f62c24d50d2d1402ac

bcf75736d176394f3df69f3e0ef7dd9f

be1f24457141d80206bc2e58f55dc879

c013f308d170aa2eca4a5b0f0bbd3ccb

c0a2fd066c955137036f92da2c3a3ff1

c17b3ec40ed5216e44311138aafaea2c

c262a39f49604f05a5656213f758cd46

c66f36eb180438882133717c3abb5157

c986c7bf720ce1463c3d628d2b3dad01

c9c16287cbbe5a037244e374ba84aecc

cbcd728a2350712b5747cd3447473deb

cbeeb123efe8cf7f842426b673415c28

ccb15eef4287c8efa472915bcb4ec458

ccdddb69e9344a039c4ac9c49a6f2d7b

cd1312be032256a10cf866af3e9afae9

ce0dd163d9e02bfd42d61024523cb134

ceef2e728db1b5ae15432f844eeb66e1

d12d98a0877f6e3c8b5a59f41cc4de9b

d131f17689f1f585e9bfdcdb72a626bb

d173076d97a0400a56c81089912b9218

d255291bb8e460626cb906ebacc670e5

d2cea317778ad6412c458a8a33b964fd

d3cfee76468a9556fd9d017c1c8ee028

d3d72f4c7038f7313ad0570e16c293bf

d485a1b5db2f97dc56500376d677aa89

d662d20507bebc37b99a4d413afa2752

d711d577b9943ab4e2f8a2e06bb963e3

d92e87d2689957765987e2be732d728e

d966c6c822122e96f6e9f5f1d4778391

daee31d7cc6e08ead6afad2175989e1d

dbb293176747fa1c2e03cbc09433f236

dc26ef761c7ec40591b1fe6e561b521d

dc9e6edeb7557bc80be68be15cebb77a

dddfbae77336120febd5ad690af3e341

e1f579227327ebb21cde3f9e7511db01

e3c642432a815a07f035e01308aaa8fc

e54329351788661f2a8d4677a759fc42

e82b7ad2c05f4617efbc86a78c1e61e9

e99cffa2afa064625f09e1c5aca8f961

ea6bd3db104ca210b5ad947d46134aaf

eb277d809a59d39d02605c0edd9333e9

ed82a50d98700179c8ae70429457477a

ef35374f4146b3532f0902d6f7f0ef8c

ef4c4d79f02ac404f47513d3a73e20c7

f05a5a60ad6f92d6f28fa4f13ded952f

f0776dfe17867709fdb0e0183ed71698

f20fbfd508e24d50522eadf0186b03eb

f3d751b0585855077b46dfce226cfea1

f4dd9bb28d680a3368136fb3755e7ea9

f804388f302af1f999e4664543c885a1

f8bcc8f99a3afde66d7f5afb5d8f1b43

```
f8d6f89aecf792e844e72015c9f27c95

f967460f8c6de1cedb180c90c98bfe98

f9d5cc0cbae77ea1a371131f62662b6b

fa4f1a3b215888bc5f19b9f91ba37519

fdff2bf247a7dad40bac228853d5a661

fe6e7fac4f0b4f25d215e28ca8a22957

fe9de1cdd645971c5d15ee1873c3ff8d

febba89b4b9a9649b3a3bf41c4c7d853
```

NCSC-NO observed the following user agents communicating with Exchange (OWA and EWS):

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36 Edg/92.0.902.67
```


NCSC-NO observed the following user agents communicating with Exchange webshell:

Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_0_1 like Mac OS X; en-us) AppleWebKit/532.9 (KHTML, like Gecko) Version/4.0.5 Mobile/8A306 Safari/6531.22.7

Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.0.7) Gecko/20060909 Firefox/1.5.0.7

Mozilla/5.0 (Linux; Android 7.0; Moto C Build/NRD90M.059) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Mobile Safari/537.36

Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.02272.101 Safari/537.36

Mozilla/5.0 (Linux; Android 5.1.1; SAMSUNG SM-J120M Build/LMY47X) AppleWebKit/537.36 (KHTML, Like Gecko) SamsungBrowser/6.4 Chrome/56.0.2924.87 Mobile Safari/537.36

Mozilla/5.0 (iPhone; CPU iPhone OS 9_0_2 like Mac OS X) AppleWebKit/601.1.45 (KHTML, like Gecko) Version/9.0 Mobile/13A452 Safari/601.1

NCSC-NO observed the following user agents communicating with Exchange Autodiscover

ExchangeServicesClient/15.00.0913.015

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36 Edg/92.0.902.67

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Firefox/114.0

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/114.0.0.0 Safari/537.36 Edg/114.0.0.0

NCSC-NO observed the following user agents communicating with EWS (/ews/Exchange.asmx):

> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.114 Safari/537.36 Edg/103.0.1264.49
>
> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36 Edg/92.0.902.67

NCSC-NO observed the following user agent communicating with Exchange (/powershell):

> Windows WinRM Client

Tags

Co-Sealers and Partners: International

MITRE ATT&CK TTP: Collection (TA0009), Command and Control (TA0011), Defense Evasion (TA0005), Discovery (TA0007), Execution (TA0002), Initial Access (TA0001), Persistence (TA0003)

Topics: Cyber Threats and Advisories </topics/cyber-threats-and-advisories>, Securing Networks </topics/cyber-threats-and-advisories/securing-networks>

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Related Advisories

JUL 31, 2025 ■ CYBERSECURITY ADVISORY | AA25-212A

CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization

</news-events/cybersecurity-advisories/aa25-212a>

JUL 22, 2025 ■ CYBERSECURITY ADVISORY | AA25-203A

#StopRansomware: Interlock

</news-events/cybersecurity-advisories/aa25-203a>

MAY 21, 2025 ■ CYBERSECURITY ADVISORY | AA25-141B

MAR 12, 2025 ■ CYBERSECURITY ADVISORY | AA25-071A

Give Feedback

[Threat Actors Deploy LummaC2 Malware to Exfiltrate Sensitive Data from Organizations </news-events/cybersecurity-advisories/aa25-141b>]

[#StopRansomware: Medusa Ransomware </news-events/cybersecurity-advisories/aa25-071a>]

Return to top

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

Give Feedback

CISA.gov
An official website of the U.S. Department of Homeland Security

Give Feedback