Hive Pro

Threat Level

Red

CISA: AA23-213A

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Ivanti Addressed Second Zero-Day Flaw Exploited by Attackers

Date of Publication

August 2, 2023

Admiralty Code

A1

TA Number

TA2023318

Summary

First Seen: Jul 28, 2023
Affected Platforms: Ivanti Endpoint Manager Mobile (EPMM)
Impact: The zero-day vulnerability (CVE-2023-35081) enables admin-authenticated attackers to write arbitrary files, risking unauthorized access, OS command execution, and malicious web shell deployment. Urgent patching is crucial to prevent widespread impact and data compromise.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-35081	Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✓	✓	✓

Vulnerability Details

#1

A new vulnerability affecting Ivanti Endpoint Manager Mobile (EPMM), previously MobileIron Core, has been identified, impacting various supported versions including releases 11.10, 11.9, and 11.8. This flaw, designated as CVE-2023-35081, allows an authenticated administrator to write arbitrary files on the EPMM server. It can be exploited alongside CVE-2023-35078 to bypass administrator authentication and restrictions, potentially leading to malicious execution of OS commands.

#2

CISA has reported that state-sponsored hackers have been exploiting these vulnerabilities since April, particularly CVE-2023-35078, which was utilized as a zero-day attack to gather data from Norwegian organizations and compromise a government agency's network. This has raised concerns about the risk of widespread exploitation in government and private networks due to the attractiveness of Mobile Device Management (MDM) systems to threat actors.

#3

The two vulnerabilities are being chained together; CVE-2023-35078, a critical authentication bypass, helps in gaining administrator access and CVE-2023-35081, a directory traversal flaw, enables arbitrary file write with the privileges of running web server. The successful attack could lead to deployment of webshells and further compromise of network.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-35081	Ivanti Endpoint Manager Mobile (formerly MobileIron Core): before 11.10.0.3	cpe:2.3:a:ivanti:mobileiron_core:*:*:*:*:*:*:*:*	CWE-22

Recommendations

Upgrade Ivanti EPMM: Promptly update Ivanti EPMM to the latest version to mitigate vulnerabilities (CVE-2023-35078 and CVE-2023-35081). Refer to Ivanti's guidance for protection details.

Secure MDM Systems: Treat Mobile Device Management (MDM) systems as high-value assets (HVAs) by implementing additional restrictions and monitoring due to their elevated access.

Follow Best Practices: Enforce multifactor authentication (MFA), adhere to cybersecurity best practices.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0011 Command and Control
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0042 Resource Development
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits	T1190 Exploit Public-Facing Application
T1087.002 Domain Account	T1087 Account Discovery	T1018 Remote System Discovery	T1036.005 Match Legitimate Name or Location
T1505.003 Web Shell	T1505 Server Software Component	T1036 Masquerading	T1070 Indicator Removal
T1005 Data from Local System	T1572 Protocol Tunneling	T1090 Proxy	T1090.001 Internal Proxy
T1059 Command and Scripting Interpreter			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	c0b42bbd06d6e25dfe8faebd735944714b421388, 1cd358d28b626b7a23b9fd4944e29077c265db46
MD5	2d5bd942ebf308df61e1572861d146f6, 473cd7cb9faa642487833865d516e578, 579ccef312d18482fc42e2b822ca2430, 849d3331f3e07a0797a02f12a6a82aa9, 8d9f7747675e24454cd9b7ed35c58707, ad55557b7cbd735c2627f7ebb3b3d493, cd08e31494f9531f560d64c695473da9, e1d8b04eeb8ef3954ec4f49267a783ef, e60dc8370ecf78cf115162fbc257baf5,

TYPE	VALUE
MD5	e669667efb41c36f714c309243f41ca7, e84a32d43db750b206cb6beed08281d0, eb5fdc72f0a76657dc6ea233190c4e1c, 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, f20fbfd508e24d50522eadf0186b03eb, f3d751b0585855077b46dfce226cfea1, f4dd9bb28d680a3368136fb3755e7ea9, f804388f302af1f999e4664543c885a1, f8bcc8f99a3afde66d7f5afb5d8f1b43, f8d6f89aecf792e844e72015c9f27c95, f967460f8c6de1cedb180c90c98bfe98, f9d5cc0cbae77ea1a371131f62662b6b, fa4f1a3b215888bc5f19b9f91ba37519, fdff2bf247a7dad40bac228853d5a661, fe6e7fac4f0b4f25d215e28ca8a22957, fe9de1cdd645971c5d15ee1873c3ff8d, febba89b4b9a9649b3a3bf41c4c7d853,

TYPE	VALUE
MD5	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,

TYPE	VALUE
MD5	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,

TYPE	VALUE
MD5	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,

TYPE	VALUE
MD5	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,

TYPE	VALUE
MD5	d92e87d2689957765987e2be732d728e, d966c6c822122e96f6e9f5f1d4778391, daee31d7cc6e08ead6afad2175989e1d, dbb293176747fa1c2e03cbc09433f236, dc26ef761c7ec40591b1fe6e561b521d, dc9e6edeb7557bc80be68be15cebb77a, dddfbae77336120febd5ad690af3e341, e1f579227327ebb21cde3f9e7511db01, e3c642432a815a07f035e01308aaa8fc, e54329351788661f2a8d4677a759fc42, e82b7ad2c05f4617efbc86a78c1e61e9, e99cffa2afa064625f09e1c5aca8f961, ea6bd3db104ca210b5ad947d46134aaf, eb277d809a59d39d02605c0edd9333e9, ed82a50d98700179c8ae70429457477a, ef35374f4146b3532f0902d6f7f0ef8c, ef4c4d79f02ac404f47513d3a73e20c7, f05a5a60ad6f92d6f28fa4f13ded952f, f0776dfe17867709fdb0e0183ed71698

Patch Details

Upgrade to the versions of Ivanti EPMM: 11.8.1.2, 11.9.1.2 and 11.10.0.3 or later versions

Link:
https://forums.ivanti.com/s/article/KB-Arbitrary-File-Write-CVE-2023-35081

References

https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write

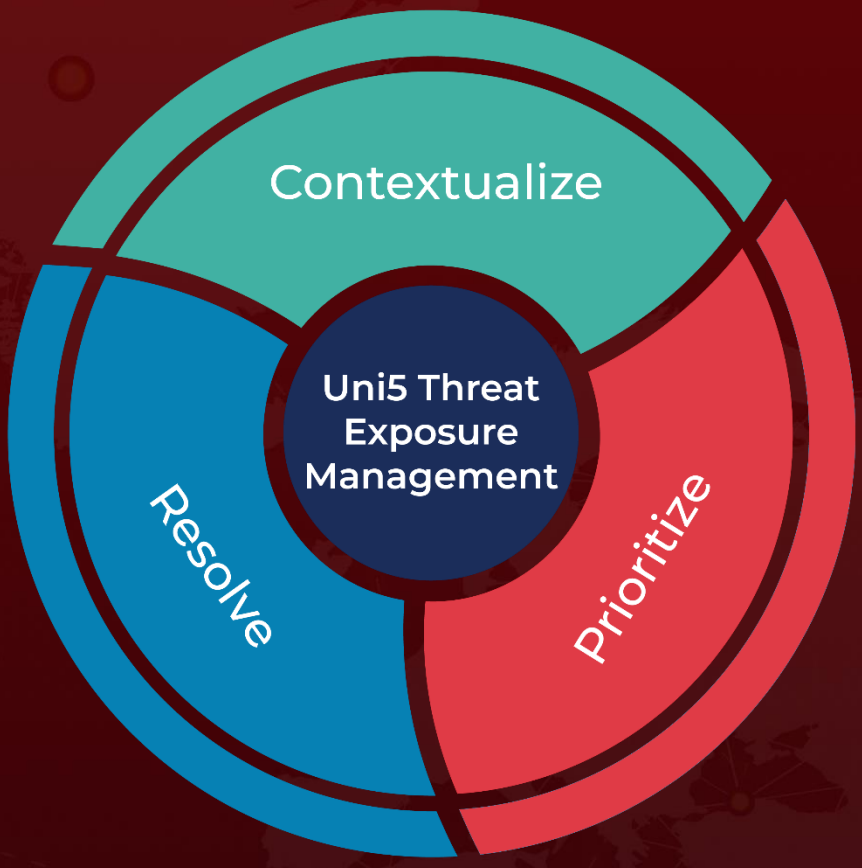
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-213a

https://www.hivepro.com/ivanti-addressed-a-critical-zero-day-flaw-in-epmm-software/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 2, 2023 . 6:30 AM

More at www.hivepro.com