Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

MinIO Vulnerabilities Exposed as Hackers Breach Through Storage

Date of Publication	Admiralty Code	TA Number
September 5, 2023	A1	TA2023353

Summary

First Seen: March 2023
Affected Product: MinIO
Impact: An elusive threat actor has been detected weaponizing critical security vulnerabilities in the MinIO high-performance object storage system, leveraging them to achieve unauthorized code execution on vulnerable servers, thereby gaining access to confidential data, executing arbitrary code, and potentially taking over servers.

⚙ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-28432	MinIO Information Disclosure Vulnerability	MinIO RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z	✗	✓	✓
CVE-2023-28434	MinIO Privilege Escalation Vulnerability	MinIO Prior to RELEASE.2023-03-20T20-16-18Z	✗	✗	✓

Vulnerability Details

#1 An unknown threat actor has been observed exploiting security vulnerabilities within the MinIO high-performance object storage system. These vulnerabilities, identified as CVE-2023-28432 and CVE-2023-28434, both categorized as high-severity issues, affect all MinIO versions prior to RELEASE.2023-03-20T20-16-18Z.

#2

The attack began with the adversaries employing social engineering tactics to convince a DevOps engineer to downgrade to an earlier, vulnerable version of the MinIO software. Subsequently, the attackers attempted to install a modified iteration of the MinIO application, named 'Evil MinIO.'

#3

As part of this nefarious operation, Evil MinIO exploits CVE-2023-28432, enabling information disclosure, and CVE-2023-28434 facilitates the replacement of the MinIO software with modified code. This manipulation introduces a backdoor accessible by appending the URL parameter 'alive' to the MinIO application's URL.

#4

After successful installation, the cybercriminals capitalized on CVE-2023-28432 to gain remote access to the server's environment variables, encompassing critical ones such as MINIO_SECRET_KEY and MINIO_ROOT_PASSWORD. The exploitation chain leverages the CVE-2023-28434 vulnerability to subvert the original .go source code file with a corrupted counterpart.

#5

After the compromise, the adversaries established a communication channel with the command and control (C2) server, through which they retrieved supplementary payloads to create profiles of the compromised hosts.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-28432	MinIO RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z	cpe:2.3:a:minio:minio:*:*:*:*:*:*:*:*	CWE-200
CVE-2023-28434	MinIO Prior to RELEASE.2023-03-20T20-16-18Z	cpe:2.3:a:minio:minio:*:*:*:*:*:*:*:*	CWE-269

Recommendations

Vulnerability Management: entails routinely assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches. Implement a protocol to ensure that DevOps teams are aware of and adapt to security upgrades.

Code Integrity and Validation: Utilize code signing and integrity checks to verify the legitimacy and integrity of software installations. Regularly validate the integrity of critical code repositories and files.

Access Control and Monitoring: Implement robust access controls and limit privileges to minimize the potential impact of an attack. Employ monitoring and alerting systems to detect unusual or unauthorized access activities. Continuously monitor for new vulnerabilities and security updates concerning third-party software and dependencies.

Data Protection and Encryption: Encrypt sensitive data both at rest and in transit to safeguard against data breaches. Maintain strong encryption keys and access controls for data security.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0007** Discovery
TA0011 Command and Control	**TA0040** Impact	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter
T1136 Create Account	**T1505.003** Web Shell	**T1082** System Information Discovery	**T1046** Network Service Discovery
T1071 Application Layer Protocol	**T1105** Ingress Tool Transfer	**T1499** Endpoint Denial of Service	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1ef7419804e401fbb3860862c2b2fbc1ec3c4650fe24fb44f787f81acf6ad65b, b14a23d0d77a45f4df4889b0c2d239fb118f9d16f944571a8b4d08603d16fb41, 9698d561de233038cf922b0de4a0bbb8e5723c800b4bc04c7ac82d92cb715dfd, 42aaacf6871108a45e1ae8ede15bc7cdcb9cf9ede067059524ba8d3b8928e91c, fc7909c24b2bb7f42648c605deacb3ae4f9574b95a562dd165e5e9aca2cc7d74, 0e084eb83954a090d83730b157f20549cf90b9d0206f5fd0bbcff009788eeafd, eadde565b44e35608447b056761ba172b608b796418ab1244607dc17d21f05e3, d56c63cc53ed72a879f224ab85019db5fc2c30e8f193c1147975d46e3f5d913a, 9e1a2a068af2524d2abc48c1edf46de8cfa3329d3688164db5969bc1914377fc, d4cf68e351992fc32021c75820f7d2a858796dd9dc245b7fbbf2cef8656081b2, 6b46cf38c45ad81dfcbbd77a1b196c5dea147088f6dab1b1920a508d61bb03ed, Fffa85e27836fd556a06660ac0ad76a35ef02687652a81194821c538e847d58f
IPv4	5[.]183[.]95[.]88
Host Name	api.timeinfo[.]org

Patch Links

https://github.com/minio/minio/security/advisories/GHSA-6xvq-wj2x-3h3q

https://github.com/minio/minio/commit/67f4ba154a27a1b06e48bfabda38355a010dfca5

References

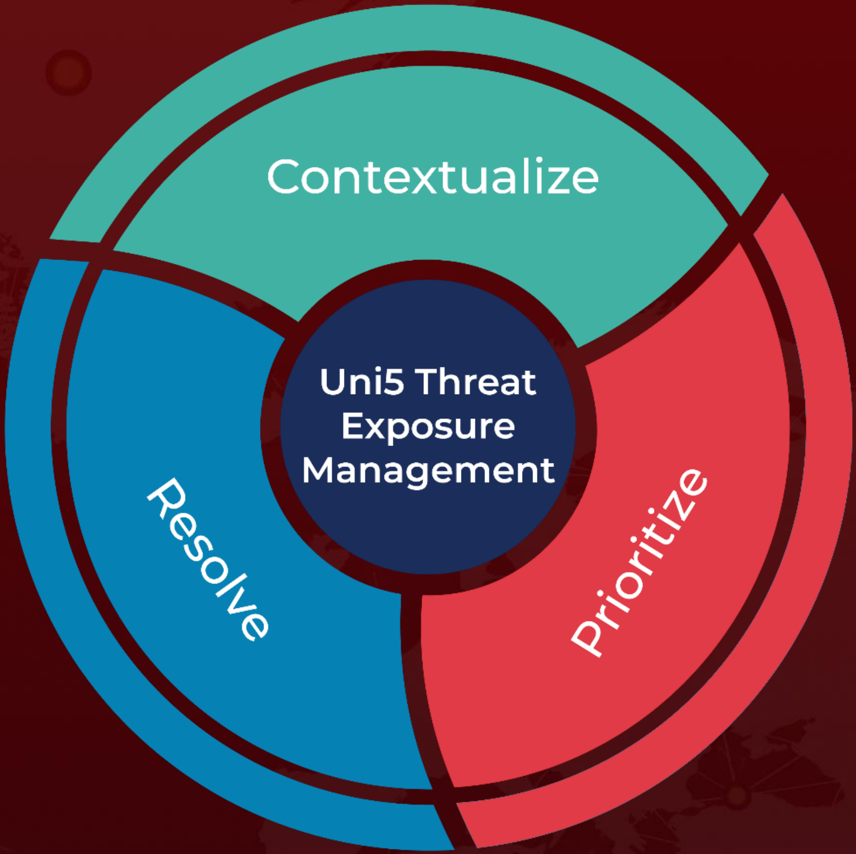
https://www.securityjoes.com/post/new-attack-vector-in-the-cloud-attackers-caught-exploiting-object-storage-services

https://www.hivepro.com/cisa-known-exploited-vulnerability-catalog-april-2023/

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

September 5, 2023 • 9:30 PM

More at www.hivepro.com