



FLASH

CLOUD SERVER MISCONFIGURATIONS

ZEROFOX INTELLIGENCE

F-2022-10-20a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Internet Infrastructure

October 20, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EDT) on October 20, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Cloud Server Misconfigurations

Key Findings

- Recent activity around BlueBleed has highlighted the prominence of cloud server misconfigurations.
- Internet-wide scanning has made it easy for exposed services to be discovered within hours of deployment.
- Many reported misconfigured servers are due to a lack of authentication.

Analyst Commentary

Misconfigured cloud servers are not a new occurrence; they happen regularly given that the ease of use of cloud servers often overshadows the need for additional security measures beyond what on-premises solutions require. These misconfigurations have garnered attention when a vulnerability is discovered or threat actors leverage them. The most recently reported event, dubbed “BlueBleed,” occurred when security researchers informed Microsoft on September 24, 2022, of a misconfigured storage endpoint allowing unauthenticated access. After being notified, Microsoft properly configured the endpoint so that it could only be accessed after authentication. Microsoft’s official response stated, “Our investigation found no indication customer accounts or systems were compromised. We have directly notified the affected customers,” in addition to expressing disappointment around the numbers listed in the report, calling them “exaggerated.”¹

With the rise of cloud computing, misconfigured cloud servers happen frequently. Unauthenticated or misconfigured AWS S3 buckets are also commonly reported. For instance, researchers found over 114 S3 buckets with a similar naming pattern in July 2021. Of those 114 buckets, 86 were accessible without any authentication. The researchers claimed that the S3 buckets affected more than 100 U.S. cities and exposed

1

[hXXps://msrc-blog.microsoft\[.\]com/2022/10/19/investigation-regarding-misconfigured-microsoft-storage-location-2/](https://msrc-blog.microsoft.com/2022/10/19/investigation-regarding-misconfigured-microsoft-storage-location-2/)



roughly one terabyte of data in over 1.6 million files.² Types of data exposed included business licenses, deeds, tax information, and personally identifiable information (PII) such as email addresses, physical addresses, phone numbers, driver's licenses, and more.

Elasticsearch instances are also commonly found to be exposed without authentication. In November 2018, a researcher using the Shodan search engine specifically to identify publicly-accessible instances of Elasticsearch discovered a server exposing over 73 gigabytes of data on U.S. citizens.³ The data contained PII such as name, email address, home address (including state and zip code), phone number, and IP address associated with the person. In addition to PII data, the server also contained an additional database with records that appeared to be related to businesses. Due to the date that the server had been indexed by Shodan, the researcher estimated that the server had been available for at least two weeks by the time it was finally taken down.

Recommendations

Internet-wide scanning capabilities have improved significantly in recent years, making it possible to easily search the entire available IPv4 address space in a reasonable amount of time for any server responding to requests from the internet. With some services indexing servers daily, it is a matter of *when*—not *if*—a public-facing server will be discovered. ZeroFox Intelligence recommends the following best practices when setting up cloud-based services:

- Regularly review access control policies.
- Ensure that all access is logged and monitored.
- Conduct thorough reviews of security settings before service deployment. Do not rely on default settings to protect data.
- Require authentication to access sensitive data.
- Consider keeping sensitive cloud services such as databases (Elasticsearch, SQL, etc.) private by not assigning public IP addresses. Cloud hosting providers often provide private networking functionality as well.
- Maintain an inventory of all cloud assets.
- Do not store PII when it is not necessary.

²

[hXXps://www.scmagazine\[.\]com/news/cloud-security/misconfigured-s3-buckets-expose-residents-data-in-more-than-80-us-municipalities](https://www.scmagazine.com/news/cloud-security/misconfigured-s3-buckets-expose-residents-data-in-more-than-80-us-municipalities)

³

[hXXps://www.zdnet\[.\]com/article/elasticsearch-server-exposed-the-personal-data-of-over-57-million-us-citizens/](https://www.zdnet.com/article/elasticsearch-server-exposed-the-personal-data-of-over-57-million-us-citizens/)



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.