November 5th, 2023 System Outage Suspicious Activities Research

REPORT

November 12th, 2023

PREPARED BY

WE THE PEOPLE AZ ALLIANCE

SUMMARY REPORT OF INCIDENT

On Sunday November 5th at about 4am az time the Maricopa Elections live feed located at https://elections.maricopa.gov/news-and-information/live-video-feeds went offline.

Later in the day 2:09pm , WTP AZ reported on X
https://twitter.com/WethePeopleAZA1/status/1721273454224187532

Also on X at 3:16pm MaricopaGOP reported the issue
https://twitter.com/MaricopaGOP/status/1721290456607470002?t=7Xormy2Gonq2TwtQpA1EUA&s=19

After the posts, Maricopa County Elections Department, later reported on X a network issue at around 4:10pm.
https://twitter.com/MaricopaVote/status/1721303926698545155

After the issue was fixed, Maricopa posted that it was fixed at 8:23pm.
https://twitter.com/MaricopaVote/status/1721367561592549714

From a technology and infrastructure stand point, it was very interesting that parts of the site went offline while other parts were still up. Also it is odd that Maricopa didn't have a redundant backup internet connection.

It was also interesting that the E-qual system, which is connected to the voter registration system, for the Arizona Secretary of State, also went down at the exact same time.

There was one very interesting and perhaps concerning find during the outage that should be investigated further:

While investigating the issue at about 7:15pm az time we discovered a hidden message in the REST API for the maricopa streaming site. The message read as the following:

"message: "java.lang.RuntimeException: org.apache.commons.dbcp.SQLNestedException: Cannot create PoolableConnectionFactory (The TCP/IP connection to the host ELC-VP-VRAS-SQL.recorder.maricopa.gov, port 1433 has failed. Error: \"connect timed out. Verify the connection properties. Make sure that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port. Make sure that TCP connections to the port are not blocked by a firewall.\".)""

What is concerning about this message is not the fact that there was an error in that connection, but what it was having an issue connecting to... **ELC-VP-VRAS-SQL.recorder.maricopa.gov, port 1433**

The site is using a public REST API and what appears to be connecting to a back- end database. The concerning part is the name of the database server connection on the back- end is named VRAS. VRAS (old voting registration and VRAS II (new version of voting registration system). This creates more questions than answers for an IT person.

How has the streaming API been programmed?

Are there other REST APIs that connect to this database server and what do they have access to?

Who has access to those REST APIs?

Why is the streaming site or any other part of the web site sharing a connection with this database server?

Does that database server have VRAS related data on it?

Where is the REST API server located onsite or offsite?

If off site, does that mean that the web streaming part and other parts of the maricopa site are reaching into an internal onsite database? Or is the database external?

These and many more questions should be asked of Maricopa County and further investigated.

Using REST APIs is a better way to limit information on sites and help protect information, but only if done correctly. It appears in this case it was not written properly because it is allowing the end user to have information about a back end internal server error.

Errors like this should be suppressed and never be shown to the public end user. This can give hints to a system that may be vulnerable or can be attacked.

Why is the Maricopa live stream using this SQL server?

For a better understanding of a REST API read the following https://www.ibm.com/topics/REST-APIs

Information on what a SQL server os https://en.wikipedia.org/wiki/Microsoft_SQL_Server