ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide additional situational awareness about recently published findings on the purchasing of a WHOIS server domain and its potential consequences.

Why this matters

A WHOIS server is an authoritative system that serves to return information about a particular network domain. Should malicious actors gain control of such a server, they can go so far as to perform a man-in-the-middle attack (MitM) on all communication going through the compromised domain.

Another potential avenue of attack is the ability to perform remote code execution (RCE) on legacy servers should these be running a vulnerable package that poorly parses WHOIS server responses.

Overview

A few days ago, security researchers published a report [1] detailing how they had discovered an expired domain, whois.dotmobiregistry.net, previously associated with the .MOBI Top Level Domain (TLD), and purchased it.

Upon setting up a WHOIS server on the newly acquired domain, they found that it was still actively queried by many systems. By September 2024, over 135,000 systems had interacted with their server, totaling 2.5 million queries. These systems included government and military mail servers, cybersecurity tools, and even Certificate Authorities (CAs) responsible for issuing SSL certificates.

The researchers theorized that by exploiting vulnerabilities in outdated WHOIS clients that parsed responses from the researchers' WHOIS server at whois.dotmobiregistry.net. Systems still querying this server, including older tools like phpWHOIS, would process maliciously crafted responses. By injecting code into these responses, the researchers could trigger RCE on vulnerable systems, allowing them to potentially execute arbitrary commands simply by controlling the server and the responses sent to the clients.

The most alarming discovery occurred when they realized CAs used their WHOIS server to verify domain ownership for certificates. This allowed the researchers to demonstrate, using a Proof of Concept (PoC), that they could manipulate CA responses, suggesting false ownership information for major domains like microsoft.mobi.

This oversight raised significant security concerns, showing that the integrity of internet communications could be undermined, particularly in cases of SSL/TLS certificates—a process already targeted by nation-states. Although they did not exploit the situation maliciously, the research highlighted vulnerabilities stemming from the outdated and fragmented WHOIS infrastructure.

Recommendations

Recommendation #1: Keep a repository of all domains registered by your organization

ORNA **strongly recommends** that organizations keep an up-to-date list of all the web domains that they have registered in order to track changes to the WHOIS and DNS servers and to the registrars themselves. This list can also be used to more easily identify all affected domains in cases such as the one presented here.

Recommendation #2: Maintain internet facing software up-to-date

ORNA **strongly recommends** that organizations maintain all systems, programs and packages that are exposed to the internet up to date in order to eliminate older vulnerabilities.

References

1. https://labs.watchtowr.com/we-spent-20-to-achieve-rce-and-accidentally-became-the-admins-of-mobi/

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.
Sincerely,
ORNA Team