



Dear Registry Operators and Registrars,

This message is to notify you of an issue regarding security exploits made possible by rogue WHOIS servers.

This notice will be available [here](#). The content of this notice follows.

Security researchers have [documented known exploits against Internet users enabled by rogue WHOIS servers](#). These rogue WHOIS servers were created by registering the expired domains of previously known WHOIS servers.

Two types of exploits have been documented. The first type of exploit uses the rogue WHOIS server to return data to [WHOIS clients with known security vulnerabilities](#), allowing remote code execution (RCE) of malware on the WHOIS clients, which may be other servers or the devices of end-users.

The second type of exploit uses the rogue WHOIS server to return false information regarding the registrant of a domain. This information may then be used to impersonate the identity of others, facilitating identity theft crimes. This exploit is possible because the WHOIS protocol has no defined method to find an authoritative WHOIS server, and therefore many WHOIS clients use inaccurate or out-of-date WHOIS server lists.

To mitigate the risk of such exploits, ICANN org strongly encourages all registry operators and registrars to maintain control of the domains of their inactive WHOIS servers indefinitely, including WHOIS servers to be decommissioned with regard to the WHOIS sunset on **28 January 2025**.

Should a registry operator or registrar no longer maintain control of a domain used for a WHOIS server, ICANN org suggests that reasonable steps should be taken to regain control of the domain. Where it is known, ICANN org has notified registry operators and registrars of domains that were previously used for WHOIS services and that should be reacquired to prevent these exploits.

ICANN org encourages everyone to use the [Registration Data Access Protocol](#) (RDAP) instead of WHOIS. RDAP has better security mechanisms than WHOIS and is less susceptible to rogue server exploits. ICANN org offers a [web-based RDAP client](#) and an [open-source, command line client](#). A list of other RDAP client implementations may be found [here](#).

Questions regarding this notice may be sent to [globalsupport@icann.org](mailto:globalsupport@icann.org).

Technical Services  
Global Domains and Strategy  
Internet Corporation for Assigned Names and Numbers (ICANN)