ISNIC PostMortem

Contents

ISNIC incident post-mortem for improper zone enumeration on 2022-01-21

At 18:33 UTC, Wednesday the 19th of January 2022 high error levels in registry website logs are flagged as suspicious.

A quick investigation confirmed that the registry website is being used in a way that is not intended. A patch was released within 24h.

No sensitive or private information was affected nor accessed. The transgressor was only able to establish that certain domain names were once registered; while ISNIC chooses not make that kind of information available, it is not considered sensitive, and some registries do publish it.

Timeline

Timestamp	Event
2022-01-17 10:15 UTC	First indications of relevant activity in the logs
2022-01-19 18:33 UTC	High level of registry website errors flagged as suspicious
2022-01-20 11:22 UTC	Software issue identified
2022-01-20 12:41 UTC	Relevant activity stops
2022-01-20 13:00 UTC	Phone conversation with the owner of the account connected to relevant activity
2022-01-20 14:45 UTC	Software issue fully patched
2022-01-20 15:16 UTC	Written explanation provided by the owner of relevant account

Event

On January 17th at 10:15 UTC a logged-in user started enumerating the `domain_id` parameter of the `/domain/overview/` endpoint on `www.isnic.is` registry website. Due to a software bug the results they got would differ for domains that are *registered* but to which they have no access (that is, for which they are not the owner, administrative contact, etc.) and for domains that had once been registered but aren't anymore.

This effectively provided them a way to learn about the fact that certain domain names were once registered but are not anymore. This information is not considered sensitive, and some registries make it explicitly available. In fact, the IETF RDAP Query Format specification (RFC7482) suggests having RDAP endpoints that provide just that information.

ISNIC, however, chooses not to – which is why this is treated as an incident.

At 18:33 UTC, Wednesday the 19th of January 2022 high error counts in registry website logs are flagged as suspicious. Further monitoring and code review leads to the discovery of the software bug, which is then fully patched within 24h, on January 21st at 14:45 UTC.

No sensitive or private information was accessed. No Essential Services were negatively affected.

Review of log data showed no other similar activity within the last few months. The affected endpoint was created within the last 9 months. Based on this we conclude with high probability that this issue has not been taken advantage of before.

ISNIC requested an explanation from the owner of the account involved in this incident. Such explanation was provided and found satisfactory.

Cause

The cause was a combination of two issues:

1. Authenticated users could display the Overview page of domains they do not control, including domain names no longer registered, by setting `domain_id` to any integer. The page would only contain the domain name as recorded in the database, and nothing more.
2. For historical reasons the domain name database field for domains that are no longer registered would contain a modified domain name. The database structure was first designed and put in production before certain advances in database technology made this approach unnecessary.

Thus, a transgressor could differentiate between the domains that are still registered and domains that had once been registered but are not registered anymore based on whether the domain name as displayed was modified or not.

A contributing factor was using an integer for `domain_id`, thus making it enumerable.

Action items/lessons learned

Certain historical design decisions proved to be conducive to this incident: a database designed today would not need to modify the domain name field of expired domain name ownership records, and would use a non-enumerable `domain_id`.

That said, updating the database structure to these modern standards would require extensive work. Due to low severity of the issue this seems uncalled for at this time, but might be a good idea long-term.