GleSYS

Falkenberg 2022-10-07

INCIDENT REPORT REGARDING DNS ISSUES

This document contains the background and remediation actions regarding our DNS service.

BACKGROUND

The GleSYS DNS service is an integral part of our hosting platform and infrastructure.

RFO

A DDoS attack from a wide number of addresses to two specific domains caused an outage in our DNS service.

SEQUENCE OF EVENTS (CEST)

2022-10-06 14:13	First automated alarm registered.
2022-10-06 14:13	Our technical staff begins troubleshooting.
2022-10-06 14:30	Issue is narrowed down to a specific domain.
2022-10-06 14:40	Implemented a block to the specific domain.
2022-10-06 14:44	Latency towards our Name Servers reached normal levels.
2022-10-06 14:46	Latency toward our Name Servers started to increase.
2022-10-06 14:46	Started to see abnormal traffic to a related domain.
2022-10-06 14:48	Same implementation was issued for this domain.
2022-10-06 14:50	Latency towards our Name Servers has once again reached normal levels.
2022-10-06 15:58	Incident at status.glesys.com updated to Monitoring.
2022-10-06 17:01	Incident at status.glesys.com updated to Resolved.
2022-10-07 13:40	Incident report published.

CONCLUSIONS SO FAR

GleSYS DNS Service is fundamental for our service delivery and incidents like this should not happen, and making sure it does not happen again is a top priority.

We have taken the following actions:

- Work has started on hardening our DNS hosting platform. The first results are expected before 2022-10-11, and all actions are expected to be completed during Q1 2023.

We would like to apologize for your problems and extra work caused by the disruption. If you as a customer have any questions or comments regarding this incident, feel free to contact us at support@glesys.se.

Sincerely,

Stefan de Vries, Head of Operations
GleSYS AB