Arizona Geological Survey National Geothermal Data System Security Upgrades

TASK 2: SECURITY UPGRADES REPORT (DRAFT)

**Overview**

One of the two primary goals of the National Geothermal Data System (NGDS) rebuild was to improve the security of its system. The need for a more secure system was prompted by a 2017 hack of the NGDS front-end that led to a multi-day service outage. To prevent similar occurrences in the future, the following steps were proposed: 1) implementation of secure hypertext transfer protocols (HTTPS) to protect against outside tampering and validate access authenticity and 2) for all NGDS servers to be rebuilt with a modern operating system that would receive security support past 2020. In addition to these two primary security upgrades, several other improvements to security were also implemented as an indirect result of upgrades to the rest of the system. Each security improvement is detailed below.

**Improvements**

*New Operating System -* A new virtual machine for the NGDS database was built using the Ubuntu 20.04 operating system. The Ubuntu 20.04 operating system is projected to continue receiving security updates and support through April 2025, after which time it will need to be replaced again.

*Implement HTTPS -* The NGDS front-end website was transferred from using the HTTP (hyper-text transfer protocol) to using HTTPS (hyper-text transfer protocol secure). HTTPS is essentially the combination of HTTP with an encryption protocol to protect traffic between the web browser and web server. In addition, we attach a certificate to the NGDS website from the University of Arizona that allows web browsers to confirm that they are making a secure connection to the true NGDS web server. These upgrades are not only important security improvements, but also improve the discoverability of NGDS because most search-engines (e.g., google) and web-browsers (e.g., google chrome) will downrank or refuse to display websites without a valid certificate and HTTPS implementation.

*Standard Firewall -*The new NGDS servers are protected by a standard firewall. The UFW firewall platform was utilized to provide host and application security protection through the Linux Kernel Netfilter framework. The primary firewalling strategy was minimizing attack surface and leaving as few cyberattack vectors open as possible. All network ports are closed except those critical to the functionality of the NGDS application, or origin-limited ports for administrative/maintenance access.

*PostgreSQL Upgrades -* The PostgreSQL database that holds NGDS catalog metadata was upgraded from version 9.1 to 12.0. Version 9.1 ceased receiving security updates in 2016 and needed to be replaced. Please visit <https://www.postgresql.org/support/security/> to see a full list of security vulnerabilities that have been fixed since the end of version 9.1. The new NGDS PostgreSQL database (v12.0) will continue to receive security updates through 2024, after which time it will need to be replaced again.

*ESRI ArcGIS Server -* The ArcGIS Enterprise server hosting many NGDS geospatial datasets was rebuilt from a 10.2 instance to 10.8. Version 10.2 ceased receiving security updates in 2017 and needed to be replaced. The new 10.8 version will continue to receive security updates through 2024, after which time it will need to be replaced again.

*New Registration Policies* - The old NGDS system allowed users to register for accounts through the CKAN API endpoint. It is through this CKAN API registration endpoint that NGDS was hacked in 2017. Registration and administrative accounts are no longer handled through the CKAN API. Account credentials are now stored and encrypted within the NGDS PostgreSQL database.

*Non-Public API -* A major unstated goal of the NGDS rebuild was to retain compatibility with the pyCSW and CKAN APIs, which are used by many other federal databases. In order to reduce public exposure, the new NGDS front-end maps all pyCSW API calls through NodeJS so that the endpoints are not visible to the public.