Table of Contents

BioStar 2, Server, Security, Hardening, Key

Allegations of BioStar 2 key exposure vulnerability

This article explains the recent allegations of BioStar 2 system having a vulnerability of protecting the system and all sensitive information.

There has been a vulnerability reported to Suprema that there is a critical issue where the information that is used to run the system can be decrypted and by this exposed data.
It has been claimed that it possible to access the database and retrieve all information that can be decrypted.

Suprema began an investigation and clarified actions described as vulnerabilities can only be demonstrated when the attacker has physical access to the server with full administrator privileges.

However, Suprema still treat these issues with extreme seriousness and priority, and with that we take responsibility to enhance the security even though the server itself has been compromised. Suprema has responded with a plan that includes more clarity and details to avoid these type of attempts.

Below are FAQs on inquiries Suprema has received :

1. How will this affect our running system?

The attack is only valid when the attacker has full access on the server. If you have hardened the server enough it is close to be impossible to experience this issue.
Please check the hardening guide for server security and review current security policies. READ MORE

2. Although it's not likely to happen, are there any solutions to apply?

BioStar 2 provides an option to store keys on a remote location. Please consider to move the keys into a safe location outside of the server that can be accessed.

3. Will this issue be not fixed?

Suprema has a plan to enhance security to implement more complicated ways that can protect the system for certain attacks directly made from the physical server itself. Over the course of the 4th quarter of 2022 and 1st quarter of 2023, BioStar 2 will be released with improved security to protect customer's valuable data.

Although these alleged vulnerabilites are only applicable if the network infrastructure is compromised, Suprema will not stop its effort to make a secure product.