Vulnerability in the Client Web Service of Lasernet 9 and older

2022-01-07 - Jason Gillan - Comments (0) - Lasernet News

During a Penetration test of Lasernet, it was identified that there is a potential file-inclusion vulnerability in one of the Client Web Services in Lasernet 9 and below.

This vulnerability is not present in Lasernet 10, and will be patched in Lasernet 9.13.3, due out next week (week starting 10th January 2022).

This vulnerability requires the Client to be enabled within the Lasernet Configuration, the attacker to have access to that endpoint, and for there to be no authentication set or for the attacker to have the authentication details already.

We strongly recommend everyone upgrades to Lasernet 10 or Lasernet 9.13.3 once it is released; however, if they are unable to upgrade but still want to remove or reduce the chance of this vulnerability getting exploited, then there are additional options that can be used, as follows:

- Disable the Client in the Lasernet Configuration
    - This will disable the endpoint that the vulnerability initially required
    - This will also disable the use of the Lasernet Client
- Secure access to the Client port via IP whitelisting in the Firewall
    - This means that only whitelisted IPs can access the Client endpoint, so the potential attacker would have to be from an approved address
- Add in Authentication
    - If “Basic Authentication + SSL Encryption” is used, it means the attacker would need to possess the credentials needed to access that endpoint and will be unable to intercept them from unsecured traffic
    - This does not prevent attackers with access to the Lasernet credentials already from performing the attack

Any or all of those above methods can help protect the affected endpoint, although the best way to ensure security of the system is to perform frequent updates to ensure the latest security patches are always applied.

If there are any further questions, or if more details are needed please contact Lasernet Support.