Security Whitepaper

Login Delay

exacqVision Server implements a login delay, in order to address the risk of various flavors of brute force attacks. More information on the nature of these attacks can be easily found elsewhere; hence, they will not be further described here.

The login delay mechanism introduces a progressive delay before completing authentication. The objective here is to increase the time required in order to carry out various flavors of intrusion attempt. The delay increases 1 second with each subsequent authentication failure, to a maximum of 26 seconds. Do note the following version-specific behaviors:

Beginning with server version 6.6.0, when login delay was first introduced, a subsequent successful login with good credentials would immediately reset the delay mechanism and emit successful login response.

Server 8.6.0 then began to apply the same delay to the first subsequent successful login as well, in keeping with security best practices (see https://cwe.mitre.org/data/definitions/307.html). However, a few ensuing problems were then observed:

1. If the delay value had increased to a large value, it would cause a Client with good credentials to arbitrarily wait for the entire delay, and give an impression of defective behavior like server or connection having stalled or otherwise become unresponsive.
2. The web service has always abandoned a connection after 10 seconds. Therefore, once the delay value had reached 10 seconds, no web service could then connect to that server unless a client were used to "unlock" the account in question, even if the web service were using correct credentials.
3. In a network arrangement where all remote clients come in via gateway and hence appear with identical IP address, one "bad" client could effectively cause a denial of service for all other remote clients.

Server 8.6.x then reduced the delay on good login to a brief duration, in order that web service would not become seemingly "locked out", and therefore would not have to be "unlocked" via another client or web service.

Created On: 8th February 2021
KB Number: KB-00138-138-210208

In a nominal scenario, users consistently log in to the server with correct username and password, and therefore would never encounter the login delay. This is made likely by virtue of the fact that ESM, Client, and the web service all persist server lists (per-user for Client, per-system for ESM and web service). Here, complications arise once a user's password has been changed, which may never occur on legacy systems with no password change enforcement. But at the same time, every new server list entry presents an opportunity for bad credential usage, and therefore at least some encounter with the login delay mechanism.