Product Security Advisory

Apache Log4j (CVE-2021-44228)

TLP:WHITE

No restriction on distribution

HID-PSA-2021-05v3

2022-January-05

Severity: CRITICAL

Overview:

A vulnerability in Apache Log4j, has been identified and is known to be under active exploitation. This vulnerability allows arbitrary code execution over a remote connection. It is very easy exploit and has been given the highest severity rating.

Affected Products

ActivClient version 7.3 where the “US Department of Defense configuration” feature has been installed (This is not installed by default.)

Note: This has no relation to the configuration “Turn on US Department of Defense configuration” within the Security Policy.

All other versions of ActivClient are unaffected.

Impact

If an attacker can send messages, even unauthenticated, to these products, they may be able to exploit the vulnerability and execute malicious code on the devices.

Mitigation

HID Global recommends users update their systems to ActivClient version 7.3.1 which is now available on the Customer Portal: https://iamsportal.hidglobal.com/products

Users may also remove the **HID Credential Management Service Client** component using the procedure provided in this document. Removal of the component will not impact ActivClient functionality. This component is installed to support future integration which are not yet released.

If neither the update nor removing the affected component can be performed, HID Global recommends users reduce access to the products until the mitigation steps can be performed. Any system remotely accessible from the internet will likely be attacked.

Contact Information:

If you have additional questions, please contact your HID representative.

If you suspect that an HID Global product has been the target of an attack, please contact HID Technical Support at https://www.hidglobal.com/support.

References:

Apache's Disclosure: https://logging.apache.org/log4j/2.x/security.html

Mitigation Procedure

For ActivClient version 7.3

On any client or server machine where ActivClient is installed:

1. From Windows Settings, open “Apps & features”
2. Select “**HID Credential Management Service Client**”
3. Select Uninstall and follow prompts to remove application
4. Restart the workstation or server

Note: Removal of the component will not impact ActivClient functionality. This component is installed to support future integration which are not yet released.