Product Security Advisory

Denial-of-Service Attacks on Bluetooth-enabled Reader Products

TLP: WHITE

No Restriction on Distribution

HID-PSA-2021-02

09-August-2021

Severity: Informational

Overview:

Awareness of Denial of Service (DoS) attacks via Bluetooth has grown and HID has opted to publish an official position on the issue with the goal of informing and educating partners and end customers.

A Denial-of-Service (DoS) attack occurs when legitimate users are unable to access systems, devices, or other resources due to the actions of a malicious threat actor. A common DoS condition can be accomplished by flooding the target device with excessive traffic until the target becomes unresponsive, and depriving legitimately authorized users of access.

In the use case of a traditional physical access control contactless reader it is possible to conduct a DoS attack by simply holding a card to the reader indefinitely, as no other credentials can be read during this time. However, this attack method has limited practical use because of the relatively short range of 125 kHz and 13.56 MHz technologies commonly used by contactless readers.

Compared to traditional contactless reader radio technologies, Bluetooth communication offers superior range and compatibility with mobile devices. However, this superior range and broad compatibility also introduces increased risk of DoS attacks because the attack can be executed covertly from greater distances. It is possible for an attacker, using off-the-shelf devices and malicious code, to repeatedly send commands to a reader, via Bluetooth, which will prevent the reader from being able to read legitimate credentials during this time.

Affected Products:

Any Bluetooth-enabled reader device is susceptible to DoS attacks. The following HID reader products include Bluetooth capability:

1. HID® iCLASS SE® Readers with a Bluetooth module
2. HID® iCLASS SE® Express Reader
3. HID® iCLASS SE® RB25F Fingerprint Reader
4. HID® Signo™ Readers

5. HID® iCLASS SE® Reader Modules with BLE Extender module
6. HID® OMNIKEY® Readers 5x27CK

Impact:

While DoS attacks can render a reader incapable of reading legitimate credentials during the attack, it is important to consider the following as you evaluate risk of such an attack within your environment:

- An attacker cannot gain unauthorized access using a DoS attack alone.
- No personal data or confidential information is exposed with a DoS attack alone.
- RFID-based DoS attacks are localized to the maximum practical range of the communication technology. But very strong or directional antennas can potentially increase the attack range beyond the specified maximum defined by communication standard (100 meters for Bluetooth).

Mitigation:

Execution of a Bluetooth-based DoS attack as described above requires Bluetooth communication. Therefore, this risk can be fully mitigated by deactivating Bluetooth communication via hardware or firmware configuration. HID has developed tools and processes that enable organizations to choose Bluetooth configuration parameters that match their security and functional requirements. HID representatives and partners are available to support end-customers who opt to deactivate Bluetooth radio communication on HID readers.

Next Steps:

Organizations which use Bluetooth readers should evaluate the risk of a DoS attack. That risk can be compared against the value and convenience that Bluetooth offers with consideration for their unique environment. HID will continue to support clients with options as it relates to Bluetooth configuration within reader products.

HID will provide updates to this issue, including additional mitigation measures if they become available, through our Security Center (https://www.hidglobal.com/security-center).

Contact Information:

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

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