Product Security Advisory

# BN_mod_sqrt() – Denial of Service

TLP:WHITE

No restriction on distribution

**HID-PSA-2022-003**

2022-May-09

**Severity:** **HIGH** - CVSS 7.5 (3.1/ AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

## Overview:

The BN_mod_sqrt() function present in OpenSSL contains a bug that can cause it to loop forever. If parsing a certificate that has invalid explicit curve parameters, a process can be subject to a denial of service attack. Since certificate parsing happens prior to verification of the certificate signature, the exploit does not require authentication.

## Affected Products:

**HID ActivID Authentication Appliance** (versions 8.4 and 8.5)

## Impact:

If exploited, the HID ActivID Authentication Appliance will not operate until it is restarted.

## Mitigation:

A hotfix for version 8.5 is available for download from the Customer Connect Portal: https://iamsportal.hidglobal.com/products

If you are using version 8.4, you must update to version 8.5 and then apply the hotfix.

HID ActivID Authentication Appliances which are forwarded the certificate from a reverse-proxy which terminates the TLS connection are not affected. However, system owners should verify the proxy system is not affected by this vulnerability.

## Contact Information:

If you have additional questions, please contact your HID Global 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:

https://www.openssl.org/news/secadv/20220315.txt

https://nvd.nist.gov/vuln/detail/CVE-2022-0778