Dimensional INSIGHT

OpenSSL 3.0.5 Vulnerabilities: CVE-2022-3786 and CVE-2022-3602

Dimensional Insight Security Office &
Dimensional Insight Research and Development Laboratory

November 1, 2022

Overview

On November 1, 2022, the OpenSSL development team released details about CVE-2022-3786 and CVE-2022-3602, two software vulnerabilities in the OpenSSL 3.0 library. Versions of DI software prior to 7.2 are not vulnerable. There is low risk to users of ProDiver 7.2. We will include OpenSSL's patch for this issue in release 7.2 (4).

Vulnerability Details

ProDiver and DiveLine use the OpenSSL library for secure communications, but only 7.2 versions of ProDiver and DiveLine use OpenSSL 3.0, and only on Windows. Software versions 6.4, 7.0, and 7.1 use earlier (non-vulnerable) versions of OpenSSL.

The OpenSSL development team has classified these defects as having a "high" severity in general (the second highest category they use.) The vulnerabilities involve certificate verification, which is only done by the client (ProDiver) contacting the server (DiveLine). Any exploit would have to involve a client contacting a malicious DiveLine server. This is an unlikely event for our customers.

DI plans to incorporate a fix in the next 7.2 release, 7.2(4), for the impacted Windows desktop programs: ProDiver, DI-Broadcast, DI-Scheduler, and DI-Config. DiveLine 7.2 for Windows will also be updated for good measure, though there is no known way to leverage the vulnerabilities via an attack on a DiveLine server.

References

- https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/

© 2022 Dimensional Insight, Inc.