OpenSSL Vulnerabilities

https://campus.barracuda.com/doc/98221683/

This article provides information about multiple vulnerabilities disclosed by the OpenSSL organization on 9th Feb 2023. The reported CVEs have various attack vectors and modalities. OpenSSL has released a security update with fixes. An attacker could exploit these vulnerabilities to take over the impacted systems.

OpenSSL is a software library for applications used to secure communications over the internet and is widely used by the majority of internet-facing HTTPS websites.

The following table provides key information about the vulnerabilities.

Table 1: Vulnerabilities and Barracuda Networks Advisory

Vulnerability	CVSS Score / Severity	Affected OpenSSL Firmware Version	Barracuda ADC Affected	Barracuda Networks Advisory
CVE-2023-0286	Awaited / High	3.0, 1.1.1 and 1.0.2	Yes	Support-assisted manual patch
CVE-2022-4304	Awaited / Moderate	3.0, 1.1.1 and 1.0.2	Yes	Support-assisted manual patch
CVE-2023-0215	Awaited / Moderate	3.0, 1.1.1 and 1.0.2	Yes	Support-assisted manual patch
CVE-2022-4450	Awaited / Moderate	3.0 and 1.1.1	Yes	Support-assisted manual patch
CVE-2022-4203	Awaited / Moderate	3.0.0 to 3.0.7	NA	Not applicable
CVE-2023-0216	Awaited / Moderate	3.0.0 to 3.0.7	NA	Not applicable
CVE-2023-0217	Awaited / Moderate	3.0.0 to 3.0.7	NA	Not applicable
CVE-2023-0401	Awaited / Moderate	3.0.0 to 3.0.7	NA	Not applicable

Exploit Description

The following section outlines a brief description of the reported vulnerabilities.

Ensure that you follow the vendor advisory for details and attack modalities.

Table 2: CVEs and Exploit Description

Number	CVE	Exploit Description
1	CVE-2023-0286	A type confusion vulnerability was found in OpenSSL when OpenSSL X.400 addresses processing inside an X.509 GeneralName. When CRL checking is enabled (for example, the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or cause a denial of service.
2	CVE-2022-4304	A timing-based side channel exists in the OpenSSL RSA Decryption implementation, which could be sufficient to recover a ciphertext across a network in a Bleichenbacher style attack.
3	CVE-2022-4203	A flaw was found in Open SSL. A read buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking.
4	CVE-2023-0215	A use-after-free vulnerability was found in OpenSSL's BIO_new_NDEF function.
5	CVE-2022-4450	A double-free vulnerability was found in OpenSSL's PEM_read_bio_ex function.
6	CVE-2023-0216	A flaw was found in OpenSSL. An invalid pointer dereference on read can be triggered when an application tries to load malformed PKCS7 data with the d2i_PKCS7(), d2i_PKCS7_bio() or d2i_PKCS7_fp() functions. This may result in an application crash which could lead to a denial of service.
7	CVE-2023-0217	A flaw was found in OpenSSL. An invalid pointer dereference on read can be triggered when an application tries to check a malformed DSA public key by the EVP_PKEY_public_check() function, most likely leading to an application crash.
8	CVE-2023-0401	A NULL pointer vulnerability was found in OpenSSL, which can be dereferenced when signatures are being verified on PKCS7 signed or signedAndEnveloped data.

Barracuda Load Balancer ADC Mitigation

Applicable for Barracuda Load Balancer ADC 540 and above:

1. CVE-2023-0286 (High) - Impacts only deployments, using Certificate Revocation Lists feature on ADC.
2. CVE-2022-4304 (Moderate) - Affects cipher suites that use RSA for key exchange.

Contact Barracuda Networks Technical Support for an assisted resolution.

Barracuda Networks Threat Research Team will update the advisory based on the evolving research data from internal as well as external threat data sources.

Recommendation

As a best practice, users of affected versions should upgrade to the version as per the list published by the vendor. Refer to Table 1 for applicable advisory on respective CVEs.

Vendor Advisory: https://www.openssl.org/news/secadv/20230207.txt

1. OpenSSL versions 3.0, 1.1.1, and 1.0.2 are vulnerable to this issue.
    1. OpenSSL 3.0 users should upgrade to OpenSSL 3.0.8.
    2. OpenSSL 1.1.1 users should upgrade to OpenSSL 1.1.1t.
    3. OpenSSL 1.0.2 users should upgrade to OpenSSL 1.0.2zg.
2. OpenSSL versions 3.0.0 to 3.0.7 are vulnerable to this issue.
    1. OpenSSL 3.0 users should upgrade to OpenSSL 3.0.8.
    2. OpenSSL 1.1.1 and 1.0.2 are not affected by this issue.

Related Articles

- https://www.hkcert.org/security-bulletin/openssl-multiple-vulnerabilities_20230209
- https://www.cisa.gov/uscert/ncas/current-activity/2023/02/09/openssl-releases-security-advisory
- https://thehackernews.com/2023/02/openssl-fixes-multiple-new-security.html
- https://digital.nhs.uk/cyber-alerts/2023/cc-4258

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.