Severity

High

Analysis Summary

CVE-2020-1968 CVSS: CVSS:3.7

The Raccoon attack exploits a flaw in the TLS specification that can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. This would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note this vulnerability only impacts DH ciphersuites and not ECDH ciphersuites.

CVE-2020-8265; CVE-2020-8287 7.2

Node.js versions prior to 10.23.1, 12.20.1, 14.15.4, 15.5.1 allow two copies of a header field in an HTTP request (for example, two transfer-encoding header fields). In this case, Node.js identifies the first header field and ignores the second. This can lead to HTTP request smuggling.

CVE-2020-8201 CVSS:6.5

Node.js < 12.18.4 and < 14.11 can be exploited to perform HTTP desync attacks and deliver malicious payloads to unsuspecting users. The payloads can be crafted by an attacker to hijack user sessions, poison cookies, perform clickjacking, and a multitude of other attacks depending on the architecture of the underlying system. The attack is possible due to a bug in processing of carrier-return symbols in the HTTP header names.

CVE-2020-8252 CVSS:7.4

The implementation of realpath in libuv < 10.22.1, < 12.18.4, and < 14.9.0 used within Node.js incorrectly determined the buffer size, which can result in a buffer overflow if the resolved path is longer than 256 bytes.

CVE-2020-8172 CVSS:7.8

TLS session reuse can lead to host certificate verification bypass in node version < 12.18.0 and < 14.4.0.

CVE-2020-8174 CVSS:8.1

napi_get_value_string_*() allows various kinds of memory corruption in node < 10.21.0, 12.18.0, and < 14.4.0.

CVE-2021-32027 CVSS:8.8

A vulnerability was found in postgresql in versions prior to 13.3, 12.7, 11.12, 10.17, and 9.6.22. While modifying certain SQL array values, missing bounds checks let authenticated database users write arbitrary bytes to a wide area of server memory. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2021-32028 CVSS:6.6

A flaw was found in postgresql. Using an INSERT … ON CONFLICT … DO UPDATE command on a purpose-crafted table, an authenticated database user could read arbitrary bytes of server memory. The highest threat from this vulnerability is to data confidentiality.

Impact

- Gain Access
- Denial of Service
- Information Disclosure

Indicators Of Compromise

CVE

- CVE-2020-1968
- CVE-2020-8265
- CVE-2020-8287
- CVE-2020-8201
- CVE-2020-8252
- CVE-2020-8172
- CVE-2020-8174
- CVE-2021-32027
- CVE-2021-32028

Affected Vendors

- Hitachi Energy

Affected Products

- SYS600: Versions 10.1.1 and prior
- SYS600: Versions 9.4 FP1 through 10.2.1
- SYS600: Versions 10.0.0 through 10.2.1

Remediation

Refer to CISA-CERT Advisory for the patch, upgrade, or suggested workaround information.

CISA-CERT Advisory