

Cyber, Forensik und Exploits

Begriffsklärung

Schwachstelle = Vulnerabilität

XXXX

Exploit

XXXX

CVE

[Common Vulnerabilities and Exposures \(Link zu Wikipedia\)](#)

The screenshot shows the CVE website interface. At the top, there is a navigation bar with links for CVE Lists, CNAs, WGs, Board, About, and News & Blog. A search bar is visible on the left. Below the navigation bar, there are buttons for 'Search CVE List', 'Downloads', 'Data Feeds', 'Update a CVE Record', and 'Request CVE IDs'. A central banner displays 'TOTAL CVE Records: 165047'. A notice below the banner states: 'NOTICE: Transition to the all-new CVE website at www.cve.org is underway and will last up to one year. (details)'. The main content area is titled 'Search Results' and indicates 'There are 49 CVE Records that match your search.' Below this, a table lists search results with columns for 'Name' and 'Description'. The first few entries are:

- CVE-2021-22156**: An integer overflow vulnerability in the calloc() function of the C runtime library of affected versions of BlackBerry® QNX Software Development Platform (SDP) version(s) 6.5.0SP1 and earlier, QNX OS for Medical 1.1 and earlier, and QNX OS for Safety 1.0.1 and earlier that could allow an attacker to potentially perform a denial of service or execute arbitrary code.
- CVE-2020-6932**: An information disclosure and remote code execution vulnerability in the slinger web server of the BlackBerry QNX Software Development Platform versions 6.4.0 to 6.6.0 could allow an attacker to potentially read arbitrary files and run arbitrary executables in the context of the web server.
- CVE-2019-8998**: An information disclosure vulnerability leading to a potential local escalation of privilege in the procs service (the /proc filesystem) of BlackBerry QNX Software Development Platform version(s) 6.3.0 SP1 and earlier could allow an attacker to potentially gain unauthorized access to a chosen process address space.
- CVE-2018-20785**: Secure boot bypass and memory extraction can be achieved on Neato Botvac Connected 2.2.0 devices. During startup, the AM335x secure boot feature decrypts and executes firmware. Secure boot can be bypassed by starting with certain commands to the USB serial port. Although a power cycle occurs, this does not completely reset the chip: memory contents are still in place. Also, it restarts into a boot menu that enables XMODEM upload and execution of an unsigned QNX IFS system image, thereby completing the bypass of secure boot. Moreover, the attacker can craft custom IFS data and write it to unused

Mitre

Abspaltung vom MIT, verwaltet die Organisation die Liste der Common Vulnerabilities and Exposures (CVE):

Wikipedia: Die MITRE Corporation ist eine Organisation zum Betrieb von Forschungsinstituten im Auftrag der Vereinigten Staaten, die durch Abspaltung vom Massachusetts Institute of Technology (MIT) entstanden ist Sie wird als Non-Profit-Organization geführt.

Killchain

XXXXX

Last
update: 2021/12/05 23:49
schulung:vulnerables_und_forensisches https://schnipsl.qgelm.de/doku.php?id=schulung:vulnerables_und_forensisches&rev=1638748149

From:
<https://schnipsl.qgelm.de/> - Qgelm

Permanent link:
https://schnipsl.qgelm.de/doku.php?id=schulung:vulnerables_und_forensisches&rev=1638748149

Last update: **2021/12/05 23:49**

