

Cyber, Forensik und Exploits

Begriffsklärung

Schwachstelle = Vulnerabilität

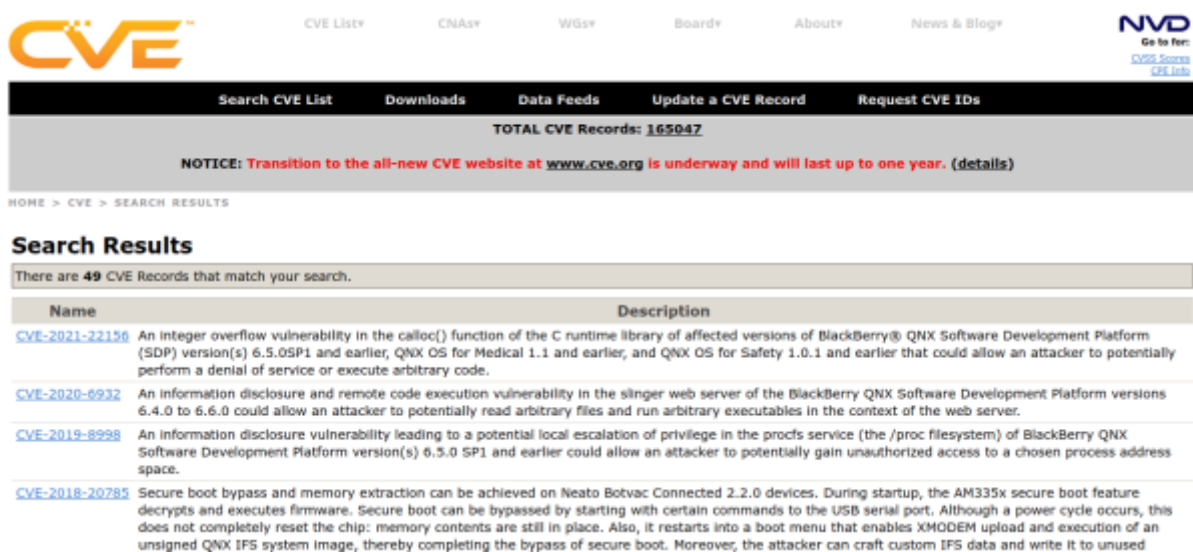
XXXX

Exploit

XXXX

CVE

Common Vulnerabilities and Exposures (Link zu Wikipedia)



The screenshot shows the CVE website interface. At the top, there's a navigation bar with links like 'CVE List', 'CNAs', 'WG's', 'Board', 'About', and 'News & Blog'. Below this is a search bar and a 'Search CVE List' button. The main content area displays 'TOTAL CVE Records: 165047' and a notice about the transition to the new CVE website at www.cve.org. Below the notice, there's a section titled 'Search Results' which states 'There are 49 CVE Records that match your search.' A table follows with columns 'Name' and 'Description'. The table lists several CVEs, including CVE-2021-22156, CVE-2020-6932, CVE-2019-8998, and CVE-2018-20785, each with a brief description of the vulnerability.

Name	Description
CVE-2021-22156	An integer overflow vulnerability in the <code>calloc()</code> 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 <code>procds</code> service (the <code>/proc</code> 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

Die Cyber Kill Chain wurde von Lockheed Martin entwickelt, um Cyberangriffe zu beschreiben. Sie

besteht aus mehreren Stufen, die ein immer tieferes Vordringen des Angreifers beschreiben.

```
<html> <p><a  
href=„https://commons.wikimedia.org/wiki/File:Intrusion\_Kill\_Chain\_-\_v2.png#/media/File:Intrusion\_Kill\_Chain\_-\_v2.png“><img  
src=„https://upload.wikimedia.org/wikipedia/commons/1/1d/Intrusion\_Kill\_Chain\_-\_v2.png“  
alt=„Intrusion Kill Chain - v2.png“></a><br>By U.S. Senate Committee on Commerce, Science, and  
Transportation - &lt;a rel=„nofollow“ class=„external free“  
href=„http://www.public.navy.mil/spawar/Press/Documents/Publications/03.26.15\_USSenate.pdf“&gt;http://www.public.navy.mil/spawar/Press/Documents/Publications/03.26.15\_USSenate.pdf&lt;/a>,,  
Public Domain, <a  
href=„https://commons.wikimedia.org/w/index.php?curid=49822676“>Link</a></p> </html>
```

From:

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

Permanent link:

https://schnipsl.qgelm.de/doku.php?id=schulung:vulnerables_und_forensisches

Last update: **2021/12/07 08:41**

