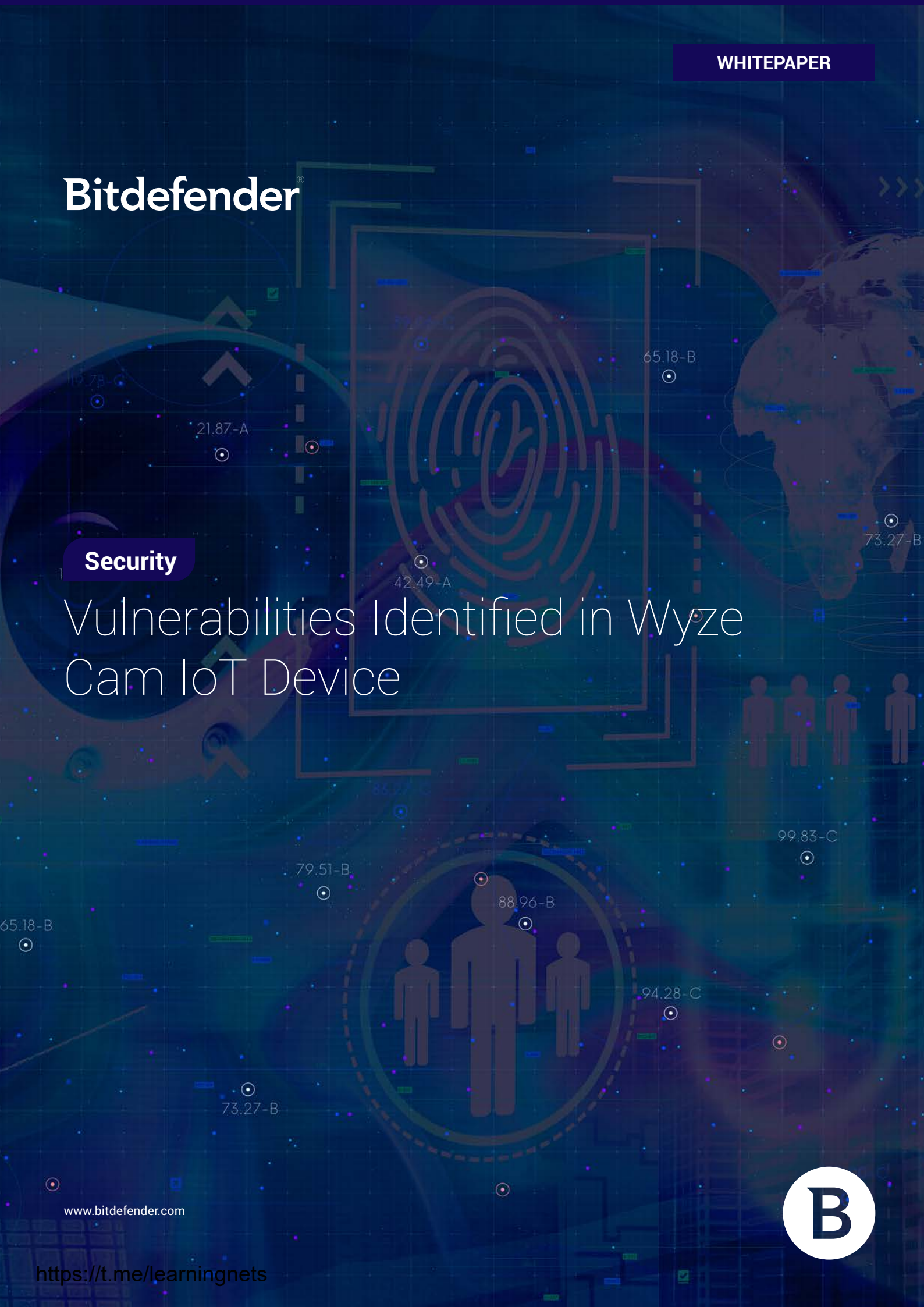
WHITEPAPER

Bitdefender



Security

Vulnerabilities Identified in Wyze Cam IoT Device

www.bitdefender.com

Contents

Foreword

At Bitdefender, we care deeply about security, so we've been working with media partners and IoT devices manufacturers to identify vulnerabilities in the world's best-selling connected devices. As a leading vendor of cybersecurity protection across endpoint and IoT devices, we have been assessing the security of smart-home equipment for more than half a decade. Our goal is to help vendors and customers stay on top of security and privacy blind spots and make the IoT ecosystem safer for everybody.

While looking into the Wyze Cam device, we identified several vulnerabilities that let an outside attacker access the camera feed or execute malicious code to further compromise the device.

IMPORTANT: The analysed device comes in several versions: Wyze Cam version 1, Wyze Cam Black version 2, as well as Wyze Cam version 3. We learned that, while versions 2 and 3 have been patched against these vulnerabilities, version 1 has been discontinued and is no longer receiving security fixes. Customers who keep using Wyze Cam version 1 are no longer protected and risk having their devices exploited.

Vulnerabilities at a glance

- Authentication bypass (**CVE-2019-9564**)
- Remote control execution flaw caused by a stack-based buffer overflow (**CVE-2019-12266)**
- Unauthenticated access to contents of the SD card

Disclosure Timeline

- Mar 06, 2019: Bitdefender makes first contact with vendor and asks PGP key via support form
- Mar 15, 2019: Bitdefender makes a second attempt at getting in touch with the vendor, still without response
- April 22, 2019 - Wyze releases updates for Wyze Cam v2 in v 4.9.4.37 and reduces risk for unauthenticated access to the contents of the SD card. Still no contact with our research team.
- April 23, 2019 - v4.10.3.50 released for Wyze Cam Pan v1 with the same risk reduction for unauthenticated access to the contents of the SD card.
- May 22, 2019: Bitdefender reserves CVE number pending publication
- September 24, 2019 - Update released for Wyze Cam v2 that fixes the CVE-2019-9564 issue.
- November 9, 2020 - Vendor fixes the CVE-2019-12266 issue with an app update.
- Nov 10, 2020: Vendor acknowledges reception and assigns an internal contact
- Nov 12, 2020: Advisory and proof of concept are shared with the vendor
- Aug 31, 2021: Bitdefender follows up on patch progress
- Sep 13, 2021: Bitdefender notifies vendor of upcoming publication
- Jan 29, 2022: Vendor releases firmware update to fix the unauthenticated access to the contents of the SD card issue.
- Mar 29, 2022: Bitdefender publishes this report

Part 1 - Remote connection authentication bypass

When connecting remotely, the client is required to log onto the device. This is usually a multi-step process, as follows:

- the client sends an IOCtl command with ID 0x2710
- the device generates a random value, encrypts it with the 16-byte “enr” and sends the result to the client
- the client, knowing “enr” value, decrypts the value and sends the result in an IOCtl command with ID 0x2712
- if the values match, the client is authenticated and is allowed to control the device

We discovered a bug in this process, which allows us to bypass the login and authenticate without knowing the “enr” value.

Normally, after the client sends the 0x2710 command, the device stores the generated value in memory. However, if we skip sending the 0x2710 command, that memory remains NULL. Then, when we send the 0x2712 command with the authentication bytes set to NULL, the device will compare NULL with NULL and authenticate us.

After authentication we can fully control the device, including motion control (pan/tilt), disabling recording to SD, turning camera on/of, among others. We can’t view the live audio and video feed, though, because it is encrypted, and the value of “enr” is unknown.

We can bypass this restriction by daisy-chaining a stack buffer overflow which leads to remote code execution (RCE) detailed in Part 2.

Part 2 - RCE from stack buffer overflow

When processing IOCtl with ID 0x2776, the device does not check whether the destination buffer is long enough before copying the contents on the stack. Exploiting this vulnerability is straight-forward.

Through the IOCtl with ID 0x2776 we can set which servers to use to connect to the cloud. This seems to be a debugging function that allows for the selection of production, beta or internal API servers. When sending a request, we specify the length of the buffer in the first byte, then the buffer itself. This content is then copied on the stack into a 0x40 bytes size buffer. Even though the specified size in the first byte is taken as signed INT, a size of 0x7F is enough to overwrite the return address of the function.

```
buffer          = -0x50
var_10          = -0x10
var_C           = -0xC
var_8           = -8
var_4           = -4

                addiu   $sp, -0x68
                li      $a2, 0x40  # '@'  # n
                sw      $s2, 0x68+var_8($sp)
                sw      $s0, 0x68+var_10($sp)
                move    $s2, $a0
                move    $s0, $a1
                addiu   $a0, $sp, 0x68+buffer  # s
                move    $a1, $zero       # c
                sw      $ra, 0x68+var_4($sp)
                jal     memset
                sw      $s1, 0x68+var_C($sp)
                lb      $s1, 0x10($s2)
                addiu   $a1, $s2, 0x11   # src
                addiu   $a0, $sp, 0x68+buffer  # dest
                move    $a2, $s1         # n
                jal     memcpy
```

Part 3 - Unauthenticated access to the contents of the SD card

When inserting an SD card into the camera, the contents of the SD card (including the recordings) can be accessed via the webserver listening on port 80 without authentication. This is due to the fact that, after an SD card is inserted, a symlink to the card mount directory is automatically created in the www directory, which is served by the webserver.

The card contents can be viewed through the hello.cgi functionality located at /cgi-bin/hello.cgi; then the files can be downloaded through the /SDPath/ path.

The SD cards also holds the camera log files. Before writing them to the card, the device XORs the content with 0x90.

These log files can contain sensitive info, such as “UID” and “enr”, which can be used to connect remotely.

Why Bitdefender

Bitdefender provides cybersecurity solutions with leading security efficacy, performance and ease of use to small and medium businesses, mid-market enterprises and consumers. Guided by a vision to be the world's most trusted cybersecurity solutions provider, Bitdefender is committed to defending organizations and individuals around the globe against cyberattacks to transform and improve their digital experience.

For more information, visit https://www.bitdefender.com.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

TECHNOLOGY ALLIANCES

Bitdefender

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-PR-WhitepaperWCorn-creat5991-en_EN
07/10/20March 23, 2022, 10:04 am03/28/22