Security Advisory 2022-067

Critical WhatsApp Vulnerabilities

September 30, 2022 — v1.0

TLP:WHITE

History:

- *30/09/2022 — v1.0 – Initial publication*

Summary

WhatsApp has patched two remote code execution vulnerabilities in its September update [1]. These could have allowed an attacker to remotely access a device and execute commands. The vulnerabilities were discovered by WhatsApp internal security team and there are no indications that these have already been exploited.

Technical Details

WhatsApp did not share more specifics on the vulnerabilities, but cybersecurity firm **Malwarebytes** said that they reside in two components called *Video Call Handler* and *Video File Handler*, which could permit an attacker to seize control of the app [3]:

- `CVE-2022-36934` - (CVSS score: 9.8) - *An integer overflow in WhatsApp could result in remote code execution (RCE) in an established video call*

An integer overflow occurs when an integer value gets assigned a value that is too large to store in the reserved representation that can be represented with a given number of digits. By writing a larger value into the memory, an attacker could overwrite other parts of the system's memory and abuse that ability to remotely execute code.

This RCE bug affects a piece of code in the WhatsApp component Video Call Handler, which allows an attacker to manipulate the bug to trigger a heap-based buffer overflow and take complete control of WhatsApp Messenger. In software exploit code, two common areas that are targeted for overflows are the stack and the heap.

The heap is an area of memory made available use by the program. The program can request blocks of memory for its use within the heap. In order to allocate a block of some size, the program makes an explicit request by calling the heap allocation operation [2].

- `CVE-2022-27492` - (CVSS score: 7.8) - *An integer underflow in WhatsApp could have caused remote code execution when receiving a crafted video file*

Integer underflow errors are usually errors that occur when a number that should always be positive gets assigned a negative value. A perfect example of an integer underflow error is when array index errors are used with a negative value. This type of weakness will lead to

undefined behavior and often crashes. In the case of overflows involving loop index variables, the likelihood of infinite loops is also high.

This RCE bug affects an unspecified code block of the component Video File Handler. The manipulation with an unknown input leads to a memory corruption vulnerability. To exploit this vulnerability, attackers would have to drop a crafted video file on the user's WhatsApp messenger and convince the user to play it [2].

Affected Products

These versions are affected by at least one of the reported vulnerabilities.

- WhatsApp for Android prior to v2.22.16.12
- WhatsApp Business for Android prior to v2.22.16.12
- WhatsApp for iOS prior to v2.22.16.12
- WhatsApp Business for iOS prior to v2.22.16.12
- WhatsApp for Android prior to v2.22.16.2 and WhatsApp for iOS v2.22.15.9 are affected by both.

Recommendations

WhatsApp has released security updates to address the reported vulnerabilities. CERT-EU recommends applying the patches as soon as possible.

References

[1] https://www.whatsapp.com/security/advisories/2022/?lang=en

[2] https://www.malwarebytes.com/blog/news/2022/09/critical-whatsapp-vulnerabilities-patched-check-youve-updated

[3] https://thehackernews.com/2022/09/critical-whatsapp-bugs-could-have-let.html