To: William H. Flathead III

From: Matteo Franzil

Subject: Security issues pt. 3: Buffer Overflow attacks

Date: October 10, 2021

This memo aims to explain the impact, the consequences and the cleanup process for the latest breach in our company.

For the third time in a row, some external actor has managed to breach our systems and exfiltrate data. However, this time the compromise has been very, very serious. Our webserver daemon had not only one, but Buffer Overflow vulnerabilities in it, and they were well used by our attackers.

Indeed, the program is flawed by its mismanagement of the size of the requests. In lines `87` and `216`, two buffers of the source code are limited to `1024` characters and no checks are made to see if data copied to those buffers actually fit the required size. While legitimate traffic usually causes no harm, people able to craft their HTTP requests are able to modify any parameter of their liking and can therefore abuse this flaw.

For example, one malevolent actor could send a request starting with `GET AAAAAA{...}AAAAAA`. As long as the string of As is longer than 1024 bytes, the buffer is smashed and the web server crashes. Of course, our issues do not limit to server crashing. Buffer Overflows allow attackers to change the flow of the affected code: since our string of copied As *overflows*, it can overwrite adjacent variables, registers, and so on. And that's what our attackers exactly did: they embedded code for spawning a root shell in the payload and used the vulnerability for executing that code.

The situation is probably more worrisome than it looks. The compromised server is probably best if burnt to the ground and completely reformatted: since the attackers had root access, we cannot be sure of what they did they do or see. Even worse, we should immediately make sure that first, attackers did not hop to neighboring machines - although the possibility of a network scan is extremely high - and second, that the root password was not used for other machines. I would say it's probably better to isolate the network as soon as possible, make a copy of the logs and launch an investigation.