To: Frobozz CEO

From: Francisco Manuel Colmenar Lamas

Subject: Webserver Buffer Overflow

Date: October 6, 2020

I am writing to inform you that the buffer overflow vulnerabilities have been found. There are two found vulnerabilities: the first in the line 87 and the second vulnerability on the line 313, both belonging to webserver.c

To patch these two vulnerabilities a file webserver.patch is provided in the submission. Its main aim is to dynamically calculate the size of the affected buffers to avoid this vulnerability.

According to the severity of the compromise, as the attacker can have full control of the server its severity is high. It is recommended to fix these vulnerabilities to avoid further damage to the company.

To restore the system to a safe state the provided patch should be applied to the webserver. Also an analysis of the users' permissions at the system should be done to discover if any user has escalated its own privileges using these vulnerabilities.

The only known consequences are the exfiltration of files from inside the company and the sending of span from the server. It is recommended to investigate where these files were sent to as well as which files were send to gain further knowledge of the current situation of the company. Furthermore, in order to stop the sending of span from the server the services run on the server should be inspected to find the ones in charge of this action and to stop them.

Please let me know if you have any more questions about this situation or its technical specification.