To: The CEO FrobozzCo

From: Evidence Monday

Date: October 9, 2019

Subject: Recently discovered threats which jeopardize webserver functionality

I am seeking approval to install several security patches which are required by your webserver running on Linux operating system. I recently discovered some buffer overflow vulnerabilities present in the currently installed version of webserver.c code. They are present in the GET and POST request headers in the code. This poses a critical threat to your webserver as any remote attacker can exploit this vulnerability.

These vulnerabilities allow attackers to crash the webserver by inserting bogus data beyond the boundaries of pre-allocated fixed length buffers. For example, in the code 'hdrval[1024]' represents a fixed array on which a malicious attacker can input bogus data beyond this array size and interrupt the normal flow of the server or crash it totally. This vulnerability can be fixed by adding a bound check before copying to buffer as seen in the patch.

Another vulnerability is found using the 'strlen' and 'strcat' function at different aspect of the webserver code. This is dangerous because there is nothing that will top a malicious user from strcat-ing more than 100 bytes into 'headername' buffers, which will in turn result in heap corruption, stack corruption and the program will eventually crash. A possible solution to fix this vulnerability is the use of 'malloc' to allocate the size of the strings to ensure count is not too big, as seen in the patch.

Failure to install or accept these patches will expose the webserver to remote code execution and leading to additional operational risk. While risk can never be fully eliminated, these patches provides the required security for FrobozzCo and ensure that the webserver remains available and secure for clients' use.

Tests with these patches have been carried out in a non-production testing environment of which the results are positive. The buffer overflow vulnerabilities have been properly mitigated and installation of these patches will not hinder normal functionalities of your critical systems.