FrobozzCo Memorandum

To: William H. Flathead III,CEO, FrobozzCo

From: Evidence Monday

Date: October 17, 2019

Subject: Recently discovered threats which jeopardize memo view and FCCU Web application.

I am seeking approval to install several security patches which are required by your memo viewing application running web browsers that can be accessed remotely or locally. I recently identified new threat vectors which jeopardize system security and could place valuable corporate data at risk for unintentional disclosure or unauthorized modification. Hence, the patch is recommended to be installed immediately.

These are path name traversal and sql injection vulnerabilities that are present in the currently installed version of memo viewing web application directory and FCCU web application respectively. These pose a critical threat to your web application because it allows any authenticated or unauthenticated users to request, view or execute file that normally they should not have access to. This is largely as a result of the presence of unsanitized HTTP request value in the code which means that the code will return whatever path/filename that is passed as a parameter.

A possible solution to fix the path traversal vulnerability is the use of path canonicalization, where input validation is added and memo.cgi\memo.pl is made non SUID-root as seen in the patch. That is, canonicalization takes any pathname provided and converts it to it simplest and truest representation. For the sql injection, we make sure inputs are properly sanitized by using parameterized queries or string escaping approach. String escape approach ensure a way of informing the SQL server if a string contains special characters. This enables the server treat it as a regular expression and not a server side command. Here, integers and strings are escaped with ‘mysql_real_escape_string’.

Failure to install or accept these patches will expose the memo viewing web application 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 web application efficiently secures clients’ sensitive data.

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