CU*Answers
6000 28th Street SE
Grand Rapids, MI
49546
800.327.3478

CU*ANSWERS
A Credit Union Service Organization

*Protocol

For Responding to Cyber Security Vulnerabilities

A Guide for Clients

First Published: October 21, 2014

Addressing **Vulnerabilities**

2014 has seen three world-wide, global vulnerabilities appear without warning. Heartbleed, Shellshock, and POODLE appeared out of nowhere, and required CU*Answers to patch systems and/or effectively disable elements of services. CU*Answers does not do so lightly, follows a protocol for doing so, and evaluates risk to credit union data. However certain issues, such as major vulnerabilities that are well-publicized, may require CU*Answers to address the vulnerability by taking a system offline. In addition, when patching a vulnerability or disabling a service or system, it is possible it will have effects beyond the scope of our original analysis. In such a case, we rely on the experiences of our clients to let us know when our security protocol results in a lost service.

When CU*Answers is aware that a service has been disabled, we will advise all of the clients affected through email or other means. CU*Answers will also provide expectations when services can be restored.

What to do if I want a Service Turned Back On for my Credit Union?

If your credit union chooses to accept the risk and wishes to have a service restored, the credit union can follow these steps:

1. Complete the Release of Liability Form (attached on the following page).
2. Have a credit union officer approve and sign the form.
3. Notify CU*Answers about the request.
4. If not already notified, CU*Answers will contact an executive officer regarding the request. Approval by an executive is needed before the service will be restored.

There are circumstances where CU*Answers will not turn on a service even if a waiver is signed. This would be a case where turning a service back on for one client could make other clients vulnerable, and these clients have not consented to having the service turned on. CU*Answers will attempt to find safe work-around solutions for clients; but this will not always be possible. As a cooperative, CU*Answers cannot turn on a service if there is risk to non-consenting clients or if there is additional risk CU*Answers might be exposed to if the service was restored.

1. [CREDIT UNION], and its officers, employees, directors, and agents, in consideration of such benefits and other good and valuable consideration, release absolutely, forever discharge, and covenant not to sue CU*ANSWERS, and its officers, employees, directors, agents, and business partners or software providers, from and concerning all liability, losses, claims, demands, actions, debts, and expenses of every name and nature for losses or other damages as a result of during, arising out of, or as a result of:

   [Describe the act or service involved in the cyber security vulnerability]

2. [CREDIT UNION] reaffirms that software and other services provided by CU*ANSWERS cannot be guaranteed to be error free, and agrees to implement reasonable processes to ensure the reliability and functionality of the software and services.

3. It is understood and agreed that this change is made in full and complete settlement and satisfaction the causes of action, claims and demands mentioned herein; that this Release contains the entire agreement between the parties; and that the terms of this Agreement are contractual and not merely a recital. Furthermore, this Release shall be binding upon the undersigned, and respective heirs, executors, administrators, personal representatives, successors and assigns. This Release shall be subject to and governed by the laws of the State of Michigan. This Release has been read and fully understood by the undersigned.

[CREDIT UNION]	CU*ANSWERS
_____	_____
[Name], [Title]	Randy Karnes, CEO
[Credit Union]	CU*Answers, A Credit Union Service Organization
October 20, 2014	October 20, 2014

CU*Answers
Security Protocol

CU*Answers has a well-defined protocol for responding to potential security emergencies. Our management follows a decision-tree to ensure that potential global vulnerabilities in our software are addressed. The process is as follows:

1. Upon report of a potential vulnerability, the CU*Answers Incident Response Team becomes involved, and individual members are assigned priorities, such as client contact, research, and communication with executive management.

2. CU*Answers performs research on the scope of the issue. The primary focus is to determine whether the issue is global, and therefore warrants removing a system from all client access until the problems can be resolved.

3. CU*Answers executive management is provided evidence, or lack thereof, of the scope of the security threat. CU*Answers management has decision-making authority on whether to remove a system from service.

4. Crisis communications are set up, when warranted. Depending on the scope of the issue, this may include a notice to all clients, or communications with just the affected credit unions.

5. When warranted, communications are sent to clients including uptime and downtime estimates for service interruptions.

6. If patches are required, these follow the same SDLC quality control testing process as other patches in the environment.