4.4 Remediation

A vulnerability can be remediated by providing a fix. Alternatively, mitigation instructions can often be developed as an interim solution.

Once the scope of the vulnerability has been adequately ascertained, it's time to prepare and test the fix (patch). The sequence of tasks tends to include identifying and isolating the vulnerability in the code; changing the code to eliminate the vulnerability; testing the changes, packaging the changes for distribution; and distributing the updated product. While the details of how to do this are often specific to the product as well as the vendor organization and its development process and are thus outside the scope of this document, we review each step in this section.

Isolating the Problem

Once a vulnerability report has been received and validated, it must be added into the work queue for the development team to isolate the underlying problem. This often requires input from developers knowledgeable in the code in order to precisely define the problem and understand its impacts.

Often a report will describe a single path to exploit a vulnerability, yet there may be other ways for an attacker to reach the same code and exploit it a different way. This makes it necessary for the developers and analysts responsible for fixing the code to explore the potential for other avenues of exploitation before zeroing in on the specific conditions found in the original report.

There is also the risk that the vulnerable code or component has been reused elsewhere. We have encountered vulnerabilities in multiple codebases that arose because a single developer worked on each project, copying the same vulnerable code into each of them.

Fix the Problem

Reporters and finders should recognize that developing, testing, and preparation of patches for deployment often requires some time. A vendor acting in good faith to ferret out the vulnerability and fix it thoroughly should usually be granted some leeway. A well-tested patch that is issued later is preferable to a prematurely released patch that creates further problems. We encourage finders, reporters, and vendors to communicate expectations *early* and *often* with respect to the status of the fix creation process as long as a vendor is responsive.

Mitigate What You Cannot Fix

In most cases, knowledge of a vulnerability leads the vendor to create and issue a fix to correct it. As a stopgap in scenarios where it may not be possible to develop a timely fix, a vendor or third party will sometimes provide advice on actions that can be taken to mitigate the effects of the vulnerability. Sometimes this advice is as simple as instructions for disabling the affected features of the system. In other cases, mitigation advice might include detailed configuration changes to be made by deployers. However, in nearly all cases a full fix for the vulnerability is preferable to mitigation advice, which should at best be treated as a temporary solution to the problem.