



# Vulnerability Disclosure Policy

**Last Update:** January 1<sup>st</sup>, 2011

This document describes Virtual Forge's Vulnerability Disclosure Policy. It will be used as the general guideline for disclosing vulnerabilities discovered by the Virtual Forge Research Team "CodeProfilers Labs" when releasing a security advisory.

Virtual Forge is only bound by its own disclosure policy. Virtual Forge does explicitly not accept any existing disclosure policies by a vendor.

It's in Virtual Forge's best interest to contribute to the continuous improvement of the security level of enterprise software used by our customers. Therefore, we believe that it's important to establish a clear procedure that should be followed by involved parties in order to minimize risks and provide a holistic solution to security threats.

Based on years of experience in the industry, we strongly believe that this approach provides the best balance for all the parties involved: vendor, customer and the general community.

## General Procedure

Upon the discovery of a new security vulnerability, the following procedure will take place:

1) Virtual Forge sends an e-mail to the vendor's public available security e-mail contact, notifying that a new vulnerability has been discovered and requests an S/MIME certificate in order to send the detailed information in encrypted form.

1.1. In case the vendor does not provide an S/MIME certificate, the information will be sent unencrypted at the vendor's risk. Virtual Forge will not be responsible for the eventual disclosure of the vulnerability information due to the use of unprotected communication channels.

1.2. In case the vendor does not answer to the original contact, two additional contact attempts will be made by Virtual Forge. This represents the best possible effort for communicating with the vendor through different channels (e.g. online forms, etc). If those contacts are also disregarded, the security advisory is published.

2) Virtual Forge sends a *Security Advisory* document to the vendor, which contains the technical information regarding the vulnerability. This document is provided with a reference to this Policy and a preset disclosure date, usually set to 21 days later.

2.1. In the case the vendor does not answer to the submission by the preset date, the security advisory is published.



3) Upon successful confirmation of the reception and analysis of the vulnerability, the vendor must provide Virtual Forge an estimated release date for the solution, which should not be longer than 45 days. Virtual Forge will post *the name of the vulnerability and estimated release date in the “Upcoming Advisories”* section of its Website.

4) While the solution is being developed, Virtual Forge will be available to provide further information or assistance to the vendor, in order to better understand the involved risks and contribute in the development of a comprehensive solution. In this process, Virtual Forge expects the vendor to provide periodic updates about the status of the case.

*4.1. In the case the vendor does not provide status updates, a request for status will be sent by Virtual Forge once a month. If the vendor does not answer to the initial status request after 14 days, an additional request will be sent. If there is no response to this second request within 14 days, the security advisory is published.*

5) Eventually, Virtual Forge will publish the security advisory containing the vulnerability information when any of the following situations takes place:

*5.1. The preset/agreed disclosure date is reached.*

*5.2. The vendor releases a security advisory/solution to its customers and/or the general public.*

*5.3. The vulnerability information is published by a third party.*

*5.4. More than 12 months from the original contact have passed.*

6) Virtual Forge expects that its researchers receive credit by the vendor for all individual vulnerabilities discovered. Should the vendor not grant proper credits to the respective researchers, then Virtual Forge will make this behavior public. Should the vendor repeatedly fail to grant proper credit to the respective researchers, then Virtual Forge rates this behavior as not acting responsibly. As a consequence, Virtual Forge may in the future release new vulnerabilities discovered in a product of the vendor directly to the public.