

## DSecRG Full Disclosure Policy (DSPolicy)

This policy is adapted version the Full Disclose Policy (RFPolicy) located at <http://www.wiretrip.net/rfp/policy.html>.

### Purpose of this policy

This policy exists to establish a guideline for interaction between researchers from DSecRG and software maintainer. It serves to quash assumptions and clearly define intentions, so that both parties may immediately and effectively gauge the problem, produce a solution, and disclose the vulnerability.

First and foremost, a wake-up call to the software maintainer: the researchers from DSecRG have chosen to NOT immediately disclose the problem, but rather make an effort to work with you. Hopefully you will respect and accept accordingly our choice.

### Policy definitions

The ISSUE is the vulnerability, problem, or otherwise reason for contact and communication.

The DSecRG is the research group from Digital Security Company (<http://dsec.ru>) submitting the ISSUE.

The MAINTAINER is the individual, group, or vendor that maintains the software, hardware, or resources that are related to the ISSUE.

The DATE OF CONTACT is the point in time when the DSecRG contacts the MAINTAINER.

All dates and times are relative to the DSecRG and Digital Security Company (GMT +03:00, Saint-Petersburg, Russia).

### Policy

1. The DSecRG will send email regarding the ISSUE to the MAINTAINER; the point in time when email is sent from the DSecRG is considered the DATE OF CONTACT.

Initial email of DSecRG regarding the ISSUE contains information about DSPolicy. If the MAINTAINER accepts DSPolicy conditions he replies this email without any additional information. If the MAINTAINER wants to suggest his own conditions he has to describe them into response email. In this case the DSecRG can accept offered conditions or not but should inform the MAINTAINER about conclusion.

It is important that the DSecRG review any documentation included with the object of the ISSUE for indication of a proper method of contact. That failing, the DSecRG should check the web site of the MAINTAINER for methods of contact. Should the DSecRG not be able to locate a suitable email address for the MAINTAINER, the DSecRG should address the ISSUE to:

security-alert@[MAINTAINER]

secure@[MAINTAINER]

security@[MAINTAINER]

support@[MAINTAINER]

info@[MAINTAINER]

admin@[MAINTAINER]

regardless of their existence. Anyone who could be deemed as a 'MAINTAINER' is encouraged to populate at least some of the above email addresses. Email auto-responses should not be considered as a message from the MAINTAINER.

2. The MAINTAINER is to be given 7 days from the DATE OF CONTACT; should no contact occur by the end of 7, the DSecRG may choose to send second email regarding the ISSUE to the MAINTAINER. Should no contact occur by the end of 14 days, the DSecRG may choose to disclose the ISSUE. Should the MAINTAINER contact the DSecRG, it is at the discretion of the DSecRG to delay disclosure past 7 days. The decision to delay should be passed upon active communication between the DSecRG and MAINTAINER.

3. Just as the MAINTAINER shouldn't ignore the DSecRG, neither should the DSecRG ignore the MAINTAINER. Requests from the MAINTAINER for help in reproducing problems or for additional information should be honored by the DSecRG. The DSecRG should help the MAINTAINER recreate the problem, if necessary. It's in the best interest of the DSecRG to help the MAINTAINER confirm the problem - otherwise, the DSecRG stands to disclose a potentially false ISSUE. The DSecRG is encouraged to delay disclosure of the ISSUE if the MAINTAINER provides feasible reasons for requiring so. Provided you cooperate with the researchers from DSecRG and keep us 'in the loop', we'll provide you with whatever time necessary to resolve the ISSUE.

4. If the MAINTAINER goes beyond 7 days without any communication to the DSecRG, the DSecRG may choose to send notification email to the MAINTAINER. Should no contact occur by the end of 14 days, the DSecRG may choose to disclose the ISSUE. The MAINTAINER is responsible for providing regular status updates (regarding the resolution of the ISSUE) at least once every 7 days. Note that it's the MAINTAINER's responsibility to do so, and not the DSecRG's responsibility to request them.

5. In respect for the DSecRG following this policy, the MAINTAINER is encouraged to provide proper credit to the DSecRG for doing so. There are proper ways to cite references, credit sources, and otherwise respect the origination of information. The MAINTAINER can use following information for credit:

Digital Security Research Group [DSecRG] (<http://dsecrg.ru>)

Email: [research@dsec.ru](mailto:research@dsec.ru)

The ISSUE provided by the DSecRG should be thought of as research. One way for commendation is to provide updates and product licenses. A lot of research is done on evaluation and trial versions of software - providing a single, full license/copy should produce little impact on the vendor, but greatly help researchers from the DSecRG. Another suggestion is to allow access to support sites/technical content.

6. The MAINTAINER is encouraged to coordinate a joint public release/disclosure with the DSecRG, so that advisories of problem and resolution can be made available together. Making the problem and solution advisories available together allow the community to have immediate access to both the problem description and the appropriate fix.

7. If the ISSUE is publicly disclosed, by a third-party, the DSecRG is encouraged to discuss the current status of the ISSUE with the MAINTAINER; based on that discussion, the DSecRG may choose to disclose the ISSUE. In that case the MAINTAINER should always credit the DSecRG for discovering the ISSUE.

8. If the MAINTAINER feels it's appropriate to alert the public of the issue, then there's no reason why the DSecRG should not. Should the MAINTAINER disclose the ISSUE, or items supporting/relating to the ISSUE (patches, fixes, etc), the DSecRG may choose to disclose the ISSUE.

9. In addition, should the DSecRG and MAINTAINER arrive at a unified resolution and disclosure, it may be of interest to contact the CVE officials (<http://cve.mitre.org>) to assign a CVE identifier to the vulnerability. Doing so allows the vulnerability to be referenced and cataloged, facilitating it's acceptance and use into the community.