

---

## DSecRG Full Disclosure Policy (DSPolicy)

Эта политика основана на политике полного разглашения Full Disclose Policy (RFPolicy) доступной по адресу <http://www.wiretrip.net/rfp/policy.html> и является ее адаптированной версией.

### Цель данной политики

Данная политика описывает принципы взаимодействия между исследователями из DSecRG и сторонними разработчиками программного обеспечения. Цель данной политики – определить намерения обеих сторон и устранить возможные разногласия в процессе оценки степени критичности проблемы, а также поиска ее решения и публикации информации в публичных источниках.

Разработчикам следует принять во внимание тот факт, что исследователи DSecRG приняли решение НЕ разглашать информацию о проблеме немедленно, а предприняли попытку взаимодействия с ними. Надеемся на Ваше понимание и уважение нашего решения.

### Определения политики

**ПРОБЛЕМА** - уязвимость либо другая причина для контакта и общения.

**DSecRG** - исследовательская группа компании Digital Security (<http://dsec.ru>), занимающаяся поиском и исследованием уязвимостей в различных программных продуктах и системах.

**ПРОИЗВОДИТЕЛЬ** - отдельный человек, группа или компания производящая программный продукт, оборудование или ресурс, в котором обнаружена ПРОБЛЕМА.

**ДАТА КОНТАКТА** - дата, когда исследователи из DSecRG связались с ПРОИЗВОДИТЕЛЕМ.

Все даты указываются относительно расположения DSecRG и Digital Security (GMT +03:00, Санкт-Петербург, Россия).

### Политика

1. DSecRG отправляет письмо относительно ПРОБЛЕМЫ непосредственно ПРОИЗВОДИТЕЛЮ. Время отправки письма от DSecRG считается ДАТОЙ КОНТАКТА.

Первое письмо от DSecRG относительно ПРОБЛЕМЫ содержит информацию о DSPolicy. Если ПРОИЗВОДИТЕЛЬ согласен с условиями DSPolicy, он может не указывать дополнительную информацию касательно принципов общения с ним. Если ПРОИЗВОДИТЕЛЬ хочет предложить свои условия общения, он должен описать их в ответе на наше письмо. В этом случае DSecRG рассмотрит предложенные условия и сообщит свое решение ПРОИЗВОДИТЕЛЮ.

---

DSecRG изучает любую информацию об объекте исследования для определения подходящего метода контакта. В случае отсутствия данной информации, DSecRG изучает web-сайт ПРОИЗВОДИТЕЛЯ для определения методов контакта. Если не было обнаружено подходящих адресов электронной почты ПРОИЗВОДИТЕЛЯ, DSecRG отправляет письма относительно ПРОБЛЕМЫ на следующие адреса:

security-alert@[ПРОИЗВОДИТЕЛЬ]

secure@[ПРОИЗВОДИТЕЛЬ]

security@[ПРОИЗВОДИТЕЛЬ]

support@[ПРОИЗВОДИТЕЛЬ]

info@[ПРОИЗВОДИТЕЛЬ]

admin@[ПРОИЗВОДИТЕЛЬ]

независимо от их существования. Каждый, кто является ПРОИЗВОДИТЕЛЕМ, должен обеспечить надлежащий способ контакта. Автоответ на письмо DSecRG не будет рассматриваться как сообщение от ПРОИЗВОДИТЕЛЯ.

2. ПРОИЗВОДИТЕЛЮ дается 7 дней с ДАТЫ КОНТАКТА на ответ. Если по истечении 7 дней ответа не последовало, DSecRG может принять решение отправить ПРОИЗВОДИТЕЛЮ повторное письмо относительно ПРОБЛЕМЫ. Если по истечении 14 дней с ДАТЫ КОНТАКТА ответа не последовало, DSecRG может принять решение опубликовать информацию о ПРОБЛЕМЕ в публичных источниках. Если производитель связывается с DSecRG, принятие решения о публикации информации по ПРОБЛЕМЕ откладывается на следующие 7 дней. Данное решение будет откладываться, пока осуществляется активное общение между DSecRG и ПРОИЗВОДИТЕЛЕМ.

3. Как ПРОИЗВОДИТЕЛЬ не должен игнорировать DSecRG, так и DSecRG не должен игнорировать ПРОИЗВОДИТЕЛЯ. Запросы ПРОИЗВОДИТЕЛЯ о помощи в объяснении и устранении ПРОБЛЕМЫ приветствуются со стороны DSecRG. Такое сотрудничество облегчает подтверждение ПРОБЛЕМЫ и предотвращает публикацию неверной информации. Сотрудничество с DSecRG обеспечит ПРОИЗВОДИТЕЛЮ предоставление любого необходимого времени для устранения ПРОБЛЕМЫ до публикации информации о ней в публичных источниках.

4. Если в течение 7 дней от ПРОИЗВОДИТЕЛЯ нет никакой информации о ходе устранения ПРОБЛЕМЫ, DSecRG может принять решение отправить ПРОИЗВОДИТЕЛЮ письмо с уведомлением. По истечении 14 дней с даты последнего контакта, DSecRG может принять решение опубликовать информацию о ПРОБЛЕМЕ в публичных источниках. ПРОИЗВОДИТЕЛЬ ответственен за предоставление информации о статусе решения ПРОБЛЕМЫ, по крайней мере, один раз в 7 дней. Отмечаем, что это ответственность ПРОИЗВОДИТЕЛЯ регулярно предоставлять данную информацию и DSecRG не должно просить об этом.

5. ПРОИЗВОДИТЕЛЬ может выказать свое уважение к DSecRG, указав в своих источниках DSecRG как исследователя ПРОБЛЕМЫ. Для этого можно использовать следующую информацию:

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

Email: research@dsec.ru

---

Информацию о ПРОБЛЕМЕ следует рассматривать как исследование. Большое количество исследований основано на оценке пробных версий программных продуктов, либо по ограниченной лицензии. По этой причине обеспечение единственной полной версией программного продукта в качестве благодарности будет огромной помощью в наших дальнейших исследованиях, также как и предоставление доступа к технической поддержке либо технической документации.

6. ПРОИЗВОДИТЕЛЬ может координировать совместный выход обновления/релиза и публикацию информации о ПРОБЛЕМЕ, что позволит сообществу получить непосредственный доступ не только к описанию ПРОБЛЕМЫ, но и к ее решению.

7. Если информация о ПРОБЛЕМЕ была опубликована третьей стороной, DSecRG связывается с ПРОИЗВОДИТЕЛЕМ для обсуждения текущего статуса ПРОБЛЕМЫ. Основываясь на этом обсуждении, DSecRG может принять решение опубликовать информацию о ПРОБЛЕМЕ в публичных источниках. В таком случае ПРОИЗВОДИТЕЛЬ должен всегда указывать DSecRG как исследователя ПРОБЛЕМЫ.

8. Если ПРОИЗВОДИТЕЛЬ решает опубликовать предварительную информацию о ПРОБЛЕМЕ в публичных источниках, нет никакой причины, почему DSecRG не может сделать также. Если ПРОИЗВОДИТЕЛЬ разглашает информацию о ПРОБЛЕМЕ или другую информацию относительно ПРОБЛЕМЫ, DSecRG может принять решение опубликовать информацию о ПРОБЛЕМЕ в публичных источниках.

9. Кроме того, при сотрудничестве между DSecRG и ПРОИЗВОДИТЕЛЕМ, представляет интерес связываться с представителями CVE (<http://cve.mitre.org>) для назначения уязвимостям, описанным в ПРОБЛЕМЕ, идентификатора CVE. Это позволит уязвимостям попасть в каталог CVE для удобства классификации и последующего использования в сообществе.