

# RE: Opinions on ClicktoSecure's Hailstorm Product

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-09/0246.html>

---

*From:* Gregory M Hoglund ([hoglund@clicktosecure.com](mailto:hoglund@clicktosecure.com))

*Date:* 09/27/01

Subject: RE: Opinions on ClicktoSecure's Hailstorm Product

Date: Wed, 26 Sep 2001 16:38:11 -0700

Message-ID: <183DF20D401B1E4E9F1C630E1D5091E2F7CE@hoogis.clicktosecure.com>

From: "Gregory M Hoglund" <[hoglund@clicktosecure.com](mailto:hoglund@clicktosecure.com)>

To: <[pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)>

Since it has been mentioned – I figured I should let you know we just released version 1.2

An eval can be downloaded from:

[http://www.clicktosecure.com/products/evaluation\\_request.htm](http://www.clicktosecure.com/products/evaluation_request.htm)

We added over 100 new test patterns to the basic set.

Since I wrote a large part of Hailstorm(TM) I figured I could throw in some feedback. First, Hailstorm has a fairly complex GUI. It's very advanced and everything is 'in your face' – this can be a small block to get over. That being said, we are working diligently on a 2.0 release that has a completely new GUI – no resemblance to the current one. The goal was to make Hailstorm easier to use. Be forewarned that this is an advanced tool before you go and try to download it.

On the upside – we have been very successful testing application-layer inputs from the network – custom ISAPI interfaces, firewall web-based admin interfaces, email servers, custom parsers for syslog and snmp events. Once an application gets into a parsing problem on user-supplied input, a great deal starts to break. That alone we have been finding denial-of-service attacks, buffer overflows, and metacharacter problems. Keep in mind this is 'black-box' – testing inputs over the network with only an idea of the code paths that are exercised behind them. On the lower side of the stack – we have also been very successful at network layer attacks. We have killed a hardware VPN and caused it to erase its firmware and reset its password to '1234', we have caused firewalls to fail open, found 'killer packets' that cause harsh resource consumption on routers and network-address translation processes, and demonstrated serious problems in 'DDOS protection appliances' – not to mention a variety of faults in multiple vendor's IDS solutions. The goal here is simple – help the

## SecurityFocus Penetration: RE: Opinions on ClicktoSecure's Hail

end-user and the software vendor find problems before the hackers do – add a little proactivity.

All in all, this tool is about saving time when your doing analysis. Everything is templated. It may not find complex security-architecture problems 8-) – but it will find those darned trivial bugs that keep showing up in Bugtraq every day...

I hope that someday software is written secure.

–Greg Hoglund  
CTO, Click To Secure, Inc.  
<http://www.clicktosecure.com>

---

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

---

- ***Previous message:*** [Brewis, Mark: "RE: Compaq Vulnerability"](#)
- ***Maybe in reply to:*** [Security News: "Opinions on ClicktoSecure's Hailstorm Product"](#)
- ***Next in thread:*** [Bill Pennington: "Re: Opinions on ClicktoSecure's Hailstorm Product"](#)
- ***Messages sorted by:*** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)