Worst of the Best of the Best

Garrett Held

Kevin Stadmeyer

July 2009

Overview

Security awards have crept into marketing materials and product web sites, often distracting the consumer from criteria that should be used to evaluate products. Overlooking valid criteria for products such as mail filtering and web application firewalls can be costly. Relying on security awards to make purchasing decisions can expose organizations to multiple, high-risk issues one would not normally expect in an “award-winning” product.

Motives and Goal

The main driver for this paper was not that Trustwave suddenly discovered that some awards are used purely for marketing and some products may still be vulnerable, but that vendors who advertise these awards lack even the most basic understanding of threats against their products and risks for their customers.

Additionally, while many people may realize that several of the awards are supplemental marketing only, it’s apparent that all awards are marketed together regardless of the criteria used. These awards often appear on the same page and may be used to confuse customers and clients.

What Awards Are Out There?

It would not be possible to cover every award in use, and the purpose of this paper is not to evaluate these awards as much as it is to warn against the use of these awards by demonstrating all products have vulnerabilities.

However, here are the awards that were considered during research:

- Info Security Products Guide
    - Global Product Excellence
    - Best Deployment Scenarios
    - Shaping Info Security Awards
- SC Magazine
    - Awards Winner
- Techworld.com
    - Security Project of the Year
- Information Security Magazine
    - Readers' Choice

How Do You Get Nominated?

The nomination process is actually a very gray area for most awards, while for others it’s a direct result of popularity. Methods range for independent evaluation to pay-for-nomination. The most “honest” methods appear to be reader’s choice awards of the type issues by “SC Magazine” and “Information Security Magazine”.

These two awards claim to be based on reader submissions (in the case of SC Magazine) or on reader selection from a provided list (in the case of Information Security Magazine).

	Web Site Claim
Info Security Products Guide[1]	Types of Nominations (For Shaping Info Security 2009): • "Individual Nomination i.e. CTO, CEO, CxO, President, VP or Director level $750.00" • "Team Nomination i.e. CTO's team, Product Management Team, Product Marketing Team, etc. $950.00" • "Customer (User of the products) /Partner i.e. your customer who is successfully using your company products or partner that helped deploy the solution successfully (VAR, Distributor, System Integrator, Retailer, etc.) whom you want to show your appreciation $1,250.00"
SC Magazine[2]	"Winners are chosen by a panel of readers who represent the circulation of SC Magazine. The Reader Trust Voting Panel is comprised of SC Magazine readers who have volunteered their time and experience to carefully consider each of the contenders in each category to cast their votes. They represent a cross-section of SC Magazine readership, which is comprised of both large, medium and small enterprises from all major vertical markets, including financial services, health care, government, retail and education. In addition to reviewing the materials provided by entrants, they have been advised to vote in each category for what they view as the solution that is the most effective at helping them to address the problems for which it was designed and that they may face in their own organizations. Voters also can take into consideration

[1] http://www.infosecurityproductsguide.com/awards/2009/2009ShapingSecurity.html

[2] http://www.scmagazineus.com/pages/section/429/

	the functionality, manageability, ease-of-use and scalability of the product or service, as well as the customer service and support provided for it. The reader trust panel also has been directed to peruse any applicable product reviews that SC Magazine has published in the last year. There will be one winner chosen per category."
Techworld.com	No information provided on the website. Trustwave is currently trying to contact the organization to determine this information.
Information Security Magazine[3]	"Information Security and SearchSecurity.com presented more than 1,600 readers with a survey of some 360 security products, divided into 18 categories. The categories and product lists were determined by Information Security and SearchSecurity.com editors, in consultation with recognized information security experts."

How Do You Win?

The two "People's Choice" style awards appeared to be the most transparent. Although the actual surveys and results are not supplied by the organizations they do go into some detail regarding the selection process. Both issue surveys to their readership and other "security and industry experts" in order to rank the nominations.

The two other organizations issue no guidance on the selection of award winners. When contacted for comment, at least one previous award winner commented (on the condition of anonymity) – "The short answer on this one is we wrote a check to get listed in their products guide, then worked it to get the award."

[3] http://searchsecurity.techtarget.com/productsOfTheYearAbout/0,294803,sid14_ayr2008,00.html

Exploits!

Data Sources and Methodology

This section will examine an award-winning product evaluation and vendor responses to Trustwave CVE submissions. Methodology for this section is based on an analysis of practical examples and experiences and should not be considered scientifically rigorous. However, the expert experience of the Trustwave team should help justify the conclusions.

Product X

Trustwave was asked to review a product, Product X, for a client's use. Due to the confidential nature of our CVE submission process, the product and awards have been sanitized; however, this product has won multiple awards. In fact, the marketing material contains a page full of awards.

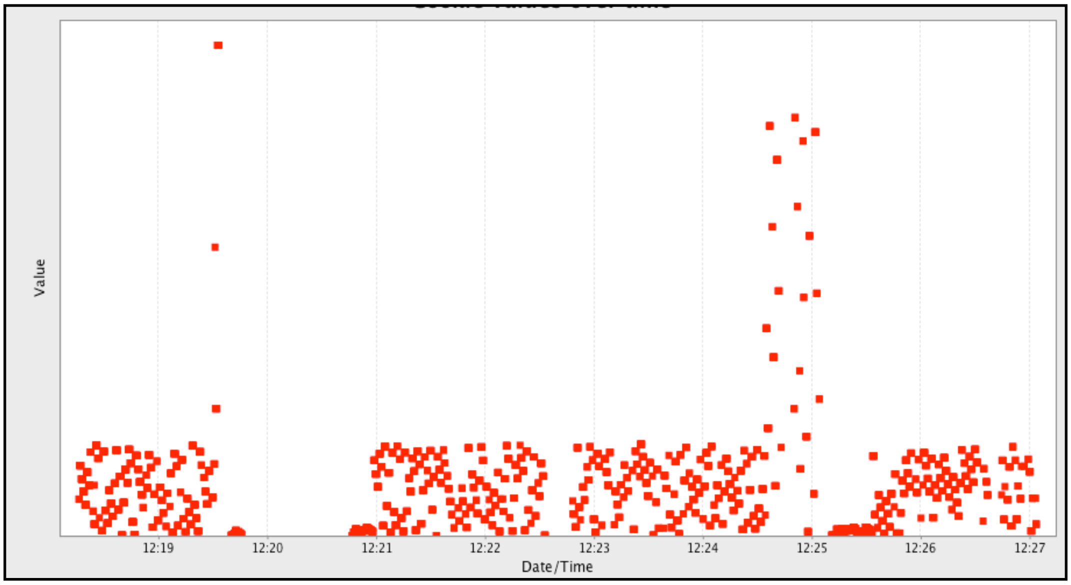
Findings

Trustwave conducted a manual application security review of the device without access to the source code. The quantity and severity of findings surprised even the testing team:

- Eight high-risk issues
- Six medium-risk issues
- Nine low-risk issues

Vulnerability Examples

- Systemic Cross-Scripting – Almost any variable was vulnerable; includes Persistent Cross-Site Scripting.
- Privilege Escalation – Changing the client-supplied (and easily predictable) user ID while in a valid session could easily result in privilege escalation.
- Custom Web Server – Resulted in the compromise of the shadow password file, and extremely poor quality root password.
- Session Hijacking – Poor implementation resulted in users able to steal sessions of users logging in around the same time of day.
- Weak Custom Session ID Algorithm:



Vendor Reaction

The findings themselves weren’t what concerned the Trustwave team - every product will probably overlook some aspect of security. What surprised the team the most was the vendor’s response, they refused to believe any of these findings were exploitable security holes.

At the time this whitepaper was submitted, the vendor has had several months of notification but still refuses to fix the vulnerabilities.

Other CVE Experiences

Trustwave has also made a push to give back to the community by focusing on CVE submissions. However, Trustwave has been met with similar reactions or a lack of action from some organizations. This includes vulnerabilities independently found by Kevin Stadmeyer, Garrett Held, and other team members that Trustwave would rank Medium and High. Because these issues are still in the process of being fixed (and have been for months) they cannot be discussed yet.

Conclusion

Based on the above practical example it should be easy to see that a lack of CVE’s does not equal security in any way, and finding metrics for evaluating products may be impossible with publicly available statistics. This is also in addition to the fact that the most popular software would also more likely be tested more often.

Lies, Damned Lies, Statistics, and Awards

Data Sources and Methodology

The four award organizations listed above were reviewed for winners of the most current award issued, the awards by year reviewed are as follows:

- SC Magazine – 2009 Awards[4]
- TechWorld.com – 2008 Awards[5]
- Info Security Products Guide – 2008 Awards [6]
- Information Security Magazine – 2008 Awards[7]

As stated in the previous section, a lack of CVE issues may be a misleading indicator of security; however Trustwave can still analyze how much turnover there is in an award category, if it's just a popularity contest, or if there's a better way to evaluate the product security process. For this last part, the theory is that a good product should have several CVE issues in the past with quick remediation timelines followed by an absence of CVE issues.

Selected Cases

Trustwave reviewed all the winners for the number of published CVE vulnerabilities (some low risk issues do not appear to be reported through CVE, where this has occurred Trustwave has relied on alternate reliable information).

Additionally, where possible Trustwave reviewed announced nominations and runners up to the awards for published CVE vulnerabilities.

The information gathered through these channels paints an interesting picture where the actual security of a product bears to relation to this award winning abilities.

Results

Our full results and statistics will be published in full during the 2009 Black Hat USA Vegas presentation. Compilation of these statistics is still in progress.

[4] http://www.scmagazineus.com/pages/section/945/

[5] http://www.techworld.com/awardswinners/

[6] http://www.infosecurityproductsguide.com/awards/index.html

[7] http://searchsecurity.techtarget.com/productsOfTheYear/0,294801,sid14_ayr2008,00.html

Preliminary analysis of select categories indicates that winning products do not contain fewer vulnerabilities then those products which did not win. In certain categories, the winning products contain far more vulnerabilities than the products which they beat out.

What Are Awards?

Just Marketing

Because there are no standard criteria and plenty of black box evaluations and pay-for-nomination processes, awards should not be considered when evaluating products. So far no award has produced a superior or inferior product recommendation compared to others.

Better Evaluations of Awards

Can any of the awards be evaluated and trusted? Probably not - they are indicators of a product's popularity among a small group of the greater security community or the marketing ability of the product team. Because the number of people qualified to make security assessments about products remains very low overall, it would be best to base decisions on other factors such as past response times and references.

Better Awards

The common saying is that "Security is a process, not a product" and it's Trustwave's belief the processes should be the focus of the awards. Time-to-patch is by far the most important statistic (in the opinion of the Trustwave research team) and it does not currently appear to be a criteria for any of the awards evaluated.