



FILE TASK

**Windows Forms Controls**  
No need to add a single line of code...

**FREE DOWNLOAD**

intent	2 days	1/17/2014	1/1	Person Name
intent	2 days	1/19/2014	1/2	Person Name
intent	2 days	1/21/2014	1/2	Person Name
intent	2 days	1/23/2014	1/2	Person Name

- [MOBILE](#)
- [CLOUD](#)
- [SECURITY](#)
- [STORAGE](#)
- [ENTERPRISE APPS](#)
- [INNOVATION](#)

Google™ Custom Search

[Android](#)
[Apple](#)
[IT Management](#)
[Networking](#)
[More](#)
[Slide Shows](#)
[Video](#)
[Blogs](#)
[Research Center](#)
[Sponsored News](#)
[RSS](#)

- [Facebook](#)
- [Twitter](#)
- [Linkedin](#)
- [Find us on Google+](#)

- [Small Business](#)
- [Virtualization](#)
- [Database Developer](#)
- [PC Hardware Servers](#)
- [eWEEKChat eWEEK at 30](#)
- [Big Data Analytics Cloud](#)
- [Backup Next Generation](#)
- [Firewall](#)

**SPONSORED NEWS**

[Big Data and the Cloud: Are Your Pipes About to Burst?](#)


[Security](#) / NSS Labs Backs Global Bountry Program to Cut Software Flaw Prevalence

# NSS Labs Backs Global Bounty Program to Cut Software Flaw Prevalence

By [Robert Lemos](#) | Posted 2013-12-19 [Email](#) [Print](#)

[Share](#) 0
 [Tweet](#) 2
 [Google +](#) 2
 [Share](#) 0
 [Like](#) 3
 [Recommend](#) 3



## An NSS Labs study proposes that software firms buy the most critical code flaws as a cost-effective way to reduce rising economic losses from cyber-crime.

Software firms' tepid approach to increasing the focus on security in the application development process has failed to staunch the flow of reports of new software flaws, but a global vulnerability purchasing program could help, argued [a report published on Dec. 18](#) by security-information firm NSS Labs.

In 2012, the number of vulnerabilities reported in software programs increased for the first time in five years and this year will likely equal or surpass that mark, according to data from the National Vulnerability Database. While the number of software flaws considered critical security threats has declined, attackers continue to have little trouble finding a software flaw to exploit.

The glut of security flaws is a prime reason that damaging digital attacks continue to plague companies, Stefan Frei, research director for NSS Labs, told *eWEEK*. While some software firms have begun training programmers in secure development techniques and using automation to catch bugs in code, most of the efforts have yet to bear fruit, Frei said.

Out of 10 major software vendors—including Adobe, Apple, IBM and Oracle—only Microsoft has reduced the number of flaws reported in its products to below its five-year and 10-year average, according to NSS Labs' data.

"On the very large scale, doing more of the same has not solved our problems," Frei said. "As it is right now, the system is fragile."



EMA: The Evolution of Data-Driven Security

[Download Now](#)

The report, which uses previous NSS Labs vulnerability analyses, estimates that a bounty program to buy serious vulnerabilities in popular software could make a dramatic difference in the cyber-criminal economy. While costing a fraction of the total cost of cyber-crime, the program could remove potential vectors of attack from the market, Frei said.



Turning Big Data Into Useful Information

## Make the most of your data

Download our eBook  
**Turning Big Data Into Useful Information**



"Today, most of the vulnerabilities are reported to the vendor for free," Frei said. "We rely 100 percent on the altruism of the researcher, while at the same time there is an expanding market from government agencies and criminals to offer extremely high rewards for the same information."

Bug bounty programs have gained increasing popularity. In 2002, iDefense [created the Vulnerability Contributor Program](#), paying security researchers for vulnerabilities in other companies' products. Since then, a number of vendors—such as Mozilla, Facebook and Google—have started rewarding researchers for bug reports. After refusing to pay for vulnerability research, Microsoft [agreed to award prizes](#) for any exploitation techniques that can bypass the defenses of the current version of Windows.

A program to buy each reported vulnerability for \$150,000—a significant bounty by today's standards—would cost \$444 million if the initiative purchased every flaw discovered in the top-50 products in 2012. While that sum may seem excessive, it represents less the 5 percent of the total cost of cyber-crime, estimated to be at least \$10 billion, NSS Labs stated in the report.

If implemented as an international program, with local groups that would receive submissions and a number of assessment centers that would randomly be assigned the task of checking the information, the program could work to remove much of the supply of vulnerabilities, Frei said.

### LATEST SECURITY ARTICLES

- [Home Depot Security Breach Affects 56M Credit Card Holders](#)
- [Bitcoin Poses Danger to British Economy, Warns Bank of England](#)
- [Home Depot Confirms Data Breach but Gives Few Details](#)
- [IBM Buys Lighthouse Security Group for Cloud-Based Identity Management](#)
- [IBM Acquires Security Software Provider CrossIdeas](#)

### [Submit a Comment](#)

There are no comments for this article yet.

Manage your Newsletters: [Login](#) [Register](#) [My Newsletters](#)

- eWeek Editor's Pick
  - News & Views
  - Cloud Computing
  - Mobile and Wireless Update
    - Best of eWeek
    - eWeek Sunday Brunch
    - eCareers Smart Moves
  - Enterprise Applications Topic Center Update
    - Enterprise IT Advantage
    - eWeek Whitepaper Spotlight
      - eWeek Labs
      - eWeek Enterprise Update
        - eWeek Storage Report
      - Industry Center Update : Finance
      - Industry Center Update : Government
      - Industry Center Update : Health Care
      - Infrastructure Topic Center Update
    - Linux & Open Source Topic Center Update
      - Mid-Market Solutions
      - Securing the Enterprise

- VoIP Topic Center Update
- What's Hot Now
- eWeekend

Safari Power Saver  
Click to Start Flash Plug-in



**MOST POPULAR**

- [News and Reviews](#)
- [Slideshows](#)
- [Home Depot Rushes to Deploy EMV Cards in Wake of Massive Data Theft](#)
- [Samsung's New Galaxy Tab S Tablets Available for Preorder by AT&T](#)
- [Microsoft Plans Early 2015 Windows Phone 9 Developer Preview](#)
- [Apple Sells 10 Million iPhone 6 Devices in First Weekend After Launch](#)

## Top White Papers and Webcasts

### Two-Factor Authentication: Evaluation Guide



One of the most foolproof ways for an online system to confirm, "Is it really you?" is by adding two-factor authentication.

Modern two-factor solutions have evolved to support new, complex technology models that change how we use data, including cloud computing and bring-your-own-device (BYOD). However, not all two-factor authentication solutions are created equal. This guide walks through some of the key area of differentiation between two-factor authentication solutions and provides some concrete criteria ...

[Download »](#)

### IDC MarketScape: Worldwide Service Desk Management Software 2014 Vendor Analysis



The rapid proliferation of tablet, mobile, and BYOD devices accessing corporate IT resources deployed on dynamic virtualized and cloud infrastructures is significantly increasing the



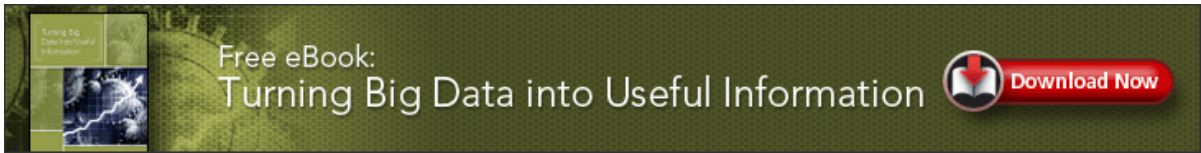
Turning Big Data Into Useful Information


an **INFOSTOR** Storage eBook

## Make the most of your data

Download our eBook  
**Turning Big Data Into Useful Information**

 [Download](#)



Free eBook:  
Turning Big Data into Useful Information 

- [Topics by Type](#)
- [Android](#)
- [Apple](#)
- [Cloud](#)
- [Database](#)
- [Developer](#)
- [Enterprise Apps](#)
- [Innovation](#)
- [IT Management](#)
  
- [Mobile](#)
- [Networking](#)
- [PC Hardware](#)
- [Security](#)
- [Servers](#)
- [Small Business](#)
- [Storage](#)
- [Virtualization](#)

- [Articles by Type](#)
- [News & Analysis](#)
- [Slideshows](#)
- [Blogs](#)
- [Reviews](#)
- [Video](#)
- 
- [Contact Us](#)
- [About eWeek](#)
- [Sitemap](#)
- [Blogs](#)
- [Security Watch](#)
- [Upfront](#)
- [First Read](#)
- [Storage Station](#)
- [Careers](#)
- [Google Watch](#)
- [Special Features](#)
- [eWeekChat](#)
- [eWeek 30th Anniversary](#)
- [Cloud Backup Project Center](#)
- [Next Generation Firewall Project Center](#)
- [Big Data Analytics Project Center](#)
- [Research Center](#)



Property of Quinstreet Enterprise.

[Terms of Service](#) | [Licensing & Reprints](#) | [Privacy Policy](#) | [Advertise](#)  
Copyright 2014 QuinStreet Inc. All Rights Reserved.