

## Security

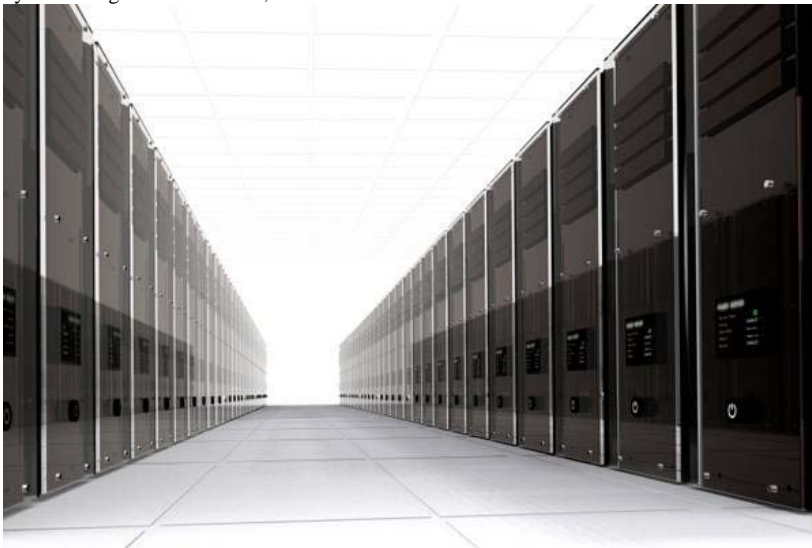
---

- [Home](#)
- [Business](#)
- [Hardware](#)
- [Software](#)
- [Security](#)
- [Internet](#)
- [Networking](#)
- [Gadgets](#)
- [Gaming](#)
- [Entertainment](#)
- [Science](#)
- [Misc](#)
- [Free Games](#)



## SourceForge offers analysis of directed server attacks

by Steve Ragan - Jan 31 2011, 13:30

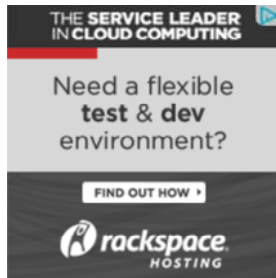


SourceForge offers analysis of directed attacks. (IMG:J.Anderson)

- [Email](#)
- [RSS](#)
- [Comment](#)
- [Facebook](#)
- [Twitter](#)
- [Digg](#)
- [FARK](#)
- [Slashdot](#)

Like

Be the first of your friends to like this.



SourceForge has invalidated user passwords for their entire community. The password resets were just part of the incident response undertaken after engineers discovered targeted attacks on the SourceForge infrastructure last Wednesday.

According to their report on the incident, SourceForge engineers discovered something strange last week, and as a precaution they started suspending services. The issue started with the servers hosting CVS services, but was determined to have spread from there.

As it turns out, someone had used a [urrw#sulylqjh](#) escalation to ultimately gain access to systems with externally faced SSH.

At this stage, SourceForge's incident response took over. The quick detection, and the segmentation of the SourceForge [qhwz run](#) itself, prevented the attack from getting out of hand. But it was determined that proper mitigation would require CVS Hosting, ViewVC, New Release deployment, and interactive shell services be suspended.

"We expect to continue work on validating data through the weekend, and begin restoring services early next week," SourceForge said in a [z hnhhgq# xsqdw](#) on the attacks.

"There is a lot of data to be validated and these tests will take some time to run. We'll provide more timeline information as we have more [lqirup dwlrc](#). We recognize that we could get services back [rqdqh](#) faster if we cut corners on data validation. We know downtime causes serious inconveniences for some of you. But given the negative consequences of corrupted data, we feel it's vital to take the time to validate everything that could potentially have been touched."

While investigating the incident, they discovered a rogue SSH Daemon that was running a password sniffing process. After killing it, SourceForge moved to invalidate all user passwords. This has forced the entire community to use email password resets in order to recover their [dffrxqw](#).

"We have no evidence to suggest that the sniffing attempt was completed successfully. But, what we definitely don't want is to find out in 2 months that passwords were compromised and we didn't take action," SourceForge explained.

The recovery process was met with confusion and harsh comments over the weekend. Initially, the recovery emails appeared to be a scam, according to some users who remarked on their "Phishy" appearance. Moreover, the reset function allows users to recycle their old, potentially compromised, passwords. Others complained that once their passwords were reset, services not shutdown due to the attack were failing to authenticate them properly.

Overall, the report from SourceForge is a good look at incident response. While the main issues were addressed and the attack was stopped from spreading, there are still problems to take care of.

What's clear is that SourceForge is willing to take the heat from parts of their community while they triple check all of their servers and recover fully. While some were displeased, the majority of the community views SourceForge's actions as commendable.

In truth, they should be commended.

SourceForge reacted swiftly. Given the scope of their [z runbj#qybrqp hqw](#) including millions of users and hundreds of thousands of projects, monitoring is no easy task. An attack like this is a needle in a haystack. Yet, they were able to locate and deal with the problem in a matter of days.

The solution isn't perfect, but it isn't supposed to be. This is why incident response is a continuously updated process.

The key, it would seem from their detailed analysis, is vigilance. They were monitoring the right points of the network at the right time. It made all the difference. The full analysis is on the SourceForge blog. [You can read it here.](#)

To reset your SourceForge password, [follow this link](#). Please use something other than your previous password.

[Comment on this Story](#)

Like

Be the first of your friends to like this.

- [Email](#)
- [RSS](#)
- [Comment](#)
- [Facebook](#)
- [Twitter](#)
- [Digg](#)
- [FARK](#)
- [Slashdot](#)

Interested in a more interactive TTH? Join our [Facebook Group](#)  
Want regular updates from The Tech Herald? [Follow us on Twitter](#)

More from the Tech Herald:



WikiLeaks knocked offline by Anonymous - Ref due Sept. 17



Occupy Wall Street protest turns chaotic and violent (Roundup)



Data intelligence firms proposed a systematic attack against WikiLeaks



Massive keylogger cache posted to Pastebin.com

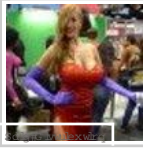


Verizon Wireless to collect and sell usage data

From around the web:



Unthinkable Poised to Happen on Wall Street. See Disturbing Charts. (Moneynews)



Comic-Con 2011 Sunday (www.redbullusa.com)



Family Scavenger Hunt with GPS Geocaching (Man of the House)



Luna di miele italiana (Rosetta Stone Blog)



Gimme Shelter: Shoe Molding and Chair Rails (HowStuffWorks Videos)

Comment on this Story

Echo 0 items

Dgp 4

**Login**

**Share**

Z kdw#q#l rxa#b lqll

Trørz

Security

- [Index](#)
- [News](#)

- [Features](#)
- [Reviews](#)



AdChoices 

**Virtual Network Security**

New PCI guidance makes security a must have in virtual environments.  
[Sourcefire.mktoweb.com](http://Sourcefire.mktoweb.com)

**SSH Clients for Windows**

Secure terminal, file transfer, and tunneling.  
Download Now!  
[www.vandyke.com](http://www.vandyke.com)

**Web Session Intelligence**

Protects your site navigation layer  
Defeat cyber-attacks in real-time  
[www.silvertailsystems.com](http://www.silvertailsystems.com)

**Secure Server With SSL**

Secure Your Site with VeriSign SSL.  
Get VeriSign SSL & Trust Seal Now!  
[www.verisign.com](http://www.verisign.com)

**In The Tech Herald**



Home  
Hardware  
Software  
Security  
Internet  
Networking  
Environments  
Science  
Current Affairs

Other Languages and Sites  
Monsters and Critics  
Deutschland (Monsters and Critics)  
Free Games Herald  
XPRNC

Site  
About Us  
Contact Us  
The Team  
RSS Feeds  
Privacy

The Fine Print  
Learn More 

© 2008 - 2011 The Tech Herald.com, TECHPUBLISH LTD. All photos are copyright their respective owners and are used under license or with permission. The Tech Herald cannot be held responsible for the content on other Web Sites.

Servers supplied by [Squint](#)

purchase directly from eligible airlines. Earn money from your site. See how 