Award-winning computer security news

# Linux distro hacked on GitHub, “all code considered compromised”

29 JUN 2018 22

Previous: The Ticketmaster brea... Next: Facebook and Google accus...

by Paul Ducklin

Data breaches are always bad news, and this one is peculiarly bad.

Gentoo, a popular distribution of Linux, has had its GitHub repository hacked.

Hacked, as in “totally pwned”, taken over, and modified; so far, no one seems to be sure quite how or why.

That’s the bad news.

Fortunately (we like to find silver linings here at Naked Security):

- The Gentoo team didn’t beat around the bush, and quickly published an unequivocal statement about the breach.
- The Gentoo GitHub repository is only a secondary copy of the main Gentoo source code.
- The main Gentoo repository is intact.

- All changes in the main Gentoo repository are digitally signed and can therefore be verified.
- As far as we know, the main Gentoo signing key is safe, so the digital signatures are reliable.

Like Drupal before it, the Gentoo team has started by assuming the worst, and figuring out how to make good from there.

That way, if things turn out to be better in practice than in theory, you’re better off, too.

Here’s what they said, less than an hour after they spotted the compromise:

> *[On] 28 June [2018] at approximately 20:20 UTC unknown individuals have gained control of the Github Gentoo organization, and modified the content of repositories as well as pages there. We are still working to determine the exact extent and to regain control of the organization and its repositories.*
>
> *All Gentoo code hosted on github should for the moment be considered compromised. This does NOT affect any code hosted on the Gentoo infrastructure. Since the master Gentoo ebuild repository is hosted on our own infrastructure*

> *and since Github is only a mirror for it, you are fine as long as you are using rsync or webrsync from gentoo.org.*
>
> *Also, the gentoo-mirror repositories including metadata are hosted under a separate Github organization and likely not affected as well.*
>
> *All Gentoo commits are signed, and you should verify the integrity of the signatures when using git.*
>
> *More updates will follow.*

If you aren’t a Linux user, you might be thinking of letting out a sly snigger round about now – you’re probably tired of hearing from the small minority of ultrafans who not only love Linux but also can’t bear to hear anything negative about any part of the Linux ecosystem.

Please don’t gloat: this isn’t about Linux, or Windows, or macOS, or any other operating system’s attitude to cybersecurity.

This breach is a reminder of the difficulty of keeping everything secure in a cloud-centric world, where you have multiple people who need the keys to the castle, multiple repositories to deal with traffic, and an apparently ever-increasing number of attackers with an enormous range of motivations for breaking into and messing with your digital stuff.

(We don’t yet know the motivtion of the attackers in this case – a grudge against Linux? a grudge against Gentoo? a grudge against Microsoft for acquiring GitHub? an attempt to spread malware? – but the reasons aren’t immediately important.)

## What to do?

Gentoo is a “build it yourself” sort of Linux distribution, where instead of downloading a set of ready-to-run files as you would with, say, Ubuntu – or macOS, or Windows, for that matter – you download the source code and compile it yourself.

The good news, of course, is that if you built it once, you can build it again – so if you fetched anything from the GitHub-hosted version of Gentoo during the danger period, get rid of it and fetch it again, using the master repository instead.

At worst, you may need or want to rebuild from scratch, bootstrapping your system from the master repository so that you’ve got a fresh start.

Then, keep your eye out for Gentoo’s official updates on what the crooks changed, and how that might have affected you during the thankfully very short window that this breach went unnoticed.

By the way, you can learn from Gentoo, even though it’s in a bit of a crisis right now:

- **Divide and conquer.** The master repository is safe, so the crooks didn’t get the crown jewels.
- **Sign everything.** Give your users a way to spot imposter files.
- **Tell the plain truth.** Say what you know, and be clear what you don’t.
- **Respond quickly.** Don’t find excuses to keep your users in the dark.

Happy recompiling 🙂

Follow @NakedSecurity 68K followers

Follow @duckblog 10.5K followers

compromise Gentoo github hack Linux

## Free tools

Sophos Home
for Windows and Mac

Hitman Pro

Sophos Mobile Security
for Android

Virus Removal Tool

Antivirus
for Linux

Previous: The Ticketmaster brea... Next: Facebook and Google accus...

## About the author

### Paul Ducklin ▸

Paul Ducklin is a passionate security proselytiser. (That's like an evangelist, but more so!) He lives and breathes computer security, and would be happy for you to do so, too.

## 22 comments on “Linux distro hacked ...

Akos June 29, 2018 at 12:54 pm

Great article as usual. As a very long-time Gentoo user, I'd like to add a few more mitigating factors:
– (I guess) most Gentoo users rsync from gentoo.org or one of its mirrors, and don't use git for updates, because rsync has always been the default. So they are not affected.
– The rsync tree is automatically verified on your own Gentoo machine by checking the GPG signatures.
– Even if you use git, all Gentoo commits are signed, so you can automatically check all merges on your machine.
So I agree with you, Gentoo's good security practices reduced the impact of this hack as much as possible.

26 1 Rate This

Reply

Aristocrates June 29, 2018 at 6:55 pm

To be fair, gentoo took a while to check GPG signatures by default (before sys-apps/portage[rsync-verify] in 2018, a default install following the handbook didn’t do any verification of the tree at all, and setting up webrsync-gpg required following a tucked away wiki page). Most major distros verify their packages with GPG out of the box by default and when I first started out years ago I erroneously took it for granted that gentoo did the same.

3 0 Rate This

Reply

aerospaceman June 29, 2018 at 3:53 pm

Forgive my ignorance, but isn’t the point of using version control to be able to track changes? If that is the case, what is the issue? Why is reverting back such an issue?

2 0 Rate This

Reply

Paul Ducklin June 29, 2018 at 6:15 pm

Well, the issue is that crooks aren't supposed to be able to access your servers and take them over, whether you are subsequently able to recover or not :-)

8 0 Rate This

Reply

Dustin Horne June 29, 2018 at 8:16 pm

Also keep in mind that control was lost on June 28th, but it’s entirely possible that the attackers had access long before that. Depending on how they got control (such as by phishing credentials), it may require a lengthy audit to figure out how long they were in the system and what modifications they could have made prior to completely taking over the repository.

6 1 Rate This

Reply

Adam June 29, 2018 at 11:00 pm

Well, with git, if you have the right permissions, you can actually erase history. Not really an issue in this case, given that these are just mirrors of the real upstream stuff, but you can make it look like something was a totally legit commit when it wasn’t (or remove commits that did specific things like patch a security flaw).

3 0 Rate This

Reply

Anonymous June 29, 2018 at 5:30 pm

regain? WTF?

0 6 Rate This

Reply

Paul Ducklin June 29, 2018 at 6:40 pm

Yes, “regain”. Not sure if you are unsure whether that’s a real English word, or unsure about its use in this context.

Seems like the right word to me: “to obtain possession or use of something after losing it.”

According to Gentoo’s own website [2018-06-29T17;37Z] , they are half-way to “regaining control”, with GitHub’s help. The imposters have been booted out and GitHub has taken control, but the account is still locked down to outside access, presumably until Gentoo and GitHub agree all the damage has been undone, whereupon I assume that GitHub will hand control back to Gentoo.

(Sounds as though they hadn’t forced all their repository users to have 2FA. Until now!)

10 1 Rate This

Reply

Jordy R June 29, 2018 at 7:00 pm

“regain” is perfect in the context

7 1 Rate This

Reply

Jimmy Sauce June 29, 2018 at 6:32 pm

How, I don’t know. Why? Because M$ bought GitHub.

0 7 Rate This

Reply

Paul Ducklin June 29, 2018 at 6:42 pm

If that really does turn out to be the motivation, then, hey, with friends like that, who needs enemies, eh?

6 1 Rate This

Reply

Aaron June 29, 2018 at 11:00 pm

Microsoft themselves are working on a Linux to replace windows. Why would they mess with GitHub they are laying the ground work to change the company. They been part of the Linux foundation for a while now

0 1 Rate This

Reply

Jack Smith June 29, 2018 at 8:12 pm

Perfect example on why to use Google ChromeOS and Crostini. Gnu/Linux and best security there is with things like this not being an issue.

1 19 Rate This

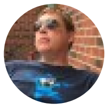
Reply

Anonymous June 29, 2018 at 9:10 pm

Niche distros rarely make head lines.

5 1 Rate This

Reply



hackspender June 29, 2018 at 10:29 pm

Kudos to the Gentoo people for announcing.

My (totally unqualified) guess is that there a good chance it's somehow related to cryptocurrency mining, and probably neither a grudge toward anyone, nor any kind of directed attack for personal reasons.

0 0 Rate This

Reply

Paul Ducklin June 30, 2018 at 5:35 pm

According to the Gentoo “debrief document” I have seen so far [2018-06-30T16:24Z], there were three separate code trees that were messed up (gentoo, musl and systemd). All of them had “rm -rf” commands (to delete everything from root or the home directory down) added into all the build scripts, thus aiming to trash the files of anyone who installed or updated any code package from those source trees. There was also a childish but offensive change made in one place, where a readme.me file was added with the text “ni**ers” in it.

So it doesn’t look like money-making cybercriminals (or so-called state actors), and it doesn’t look like anything as structured as cryptojacking. It really does look like a “screw you because we can” kind of thing… not that a fact like that exonerates or justifies anything, or makes it less criminal, of course.

6 0 Rate This

Reply

Epic_Null July 1, 2018 at 5:54 pm

Well, good news is that because they used rm, any existing data may be recoverable with an undelete software?

0 0 Rate This

Reply

Paul Ducklin July 1, 2018 at 11:30 pm

I wouldn’t bank on an undelete working very well – a backup is the best way to recover from disk disasters…

OTOH the unauthorised changes were taken offline pretty quickly and (as mentioned in the first comment) very few Gentoo users would be automatically pulling ebuild scripts from the GitHub repository anyway. I haven’t heard and stories of anyone actually being affected by the “rm” Trojanisation.

1 0 Rate This

Reply

Anonymous June 29, 2018 at 10:45 pm

“letting out a sly snigger” … umm

3 1 Rate This

Reply

a@a.com June 30, 2018 at 4:48 am

Didn’t Microsoft just buy Github? Probably not related.

0 0 Rate This

Reply

Anonymous June 30, 2018 at 5:21 am

Organization owners on GitHub can enforce 2FA for members. This should become more of a standard practice!

2 0 Rate This

Reply

Paul Ducklin June 30, 2018 at 5:23 pm

Apparently Gentoo is forcing everyone who has GitHub access to use 2FA…

….now.

Coulda, shoulda, woulda…

5 0 Rate This

Reply

## Leave a Reply

Enter your comment here...

## Recommended reads

AUG
10 BY PAUL DUCKLIN 9

How one man could have hacked every Mac developer (73% of them, anyway)

JUL
13 BY PAUL DUCKLIN 5

Linux, malware and data breaches – what can we learn? [VIDEO]

About Naked Security
About Sophos
Send us a tip
Cookies
Privacy
Legal

NETWORK PROTECTION

XG Firewall
UTM
Secure Wi-Fi
Secure Web Gateway
Secure Email Gateway

ENDUSER PROTECTION

Enduser Protection
Bundles
Endpoint Antivirus
Sophos Cloud
Mobile Control
SafeGuard Encryption

SERVER PROTECTION

Virtualization Security
Server Security
SharePoint Security
Network Storage Antivirus
PureMessage