Cisco Removed Its Seventh Backdoor Account This Year, and That's a Good Thing (zdnet.com)

Posted by BeauHD on Thursday November 08, 2018 @07:10PM from the good-on-you dept.

An anonymous reader quotes a report from ZDNet: *Cisco, the world's leading provider of top networking equipment and enterprise software, has released today 15 security updates, including a fix for an issue that can be described as a backdoor account. This latest patch marks the seventh time this year when Cisco has removed a backdoor account from one of its products. Five of the seven backdoor accounts were discovered by Cisco's internal testers, with only CVE-2018-0329 and this month's CVE-2018-15439 being found by external security researchers. The company has been intentionally and regularly combing the source code of all of its software since December 2015, when it started a massive internal audit. Cisco started that process after security researchers found what looked to be an intentional backdoor in the source code of ScreenOS, the operating system of Juniper, one of Cisco's rivals.*

Juniper suffered a massive reputational damage following the 2015 revelation, and this may secretly be the reason why Cisco has avoided using the term "backdoor account" all year for the seven "backdoor account" issues. Instead, Cisco opted for more complex wordings such as "undocumented, static user credentials for the default administrative account," or "the affected software enables a privileged user account without notifying administrators of the system." It is true that using such phrasings might make Cisco look disingenuous, but let's not forget that Cisco has been ferreting these backdoor accounts mainly on its own, and has been trying to fix them without scaring customers or impacting its own stock price along the way.

cisco os security

→
Vulnerability Could Make DJI Drones a Spy In the Sky
DOJ: Strong Encryption That We Don't Have Access To Is 'Unreasonable'
Recruiters Are Still Complaining About No-Shows At Interviews
Should Developers Abandon Agile?
Hackers Who Attended Black Hat and DefCon Conferences Say Hotel Security Personnel Demanded Access To Their Rooms
'Kernel Memory Leaking' Intel Processor Design Flaw Forces Linux, Windows Redesign
Submission: Cisco Removed Its Seventh Backdoor Account This Year, And That's A Good Thing
Google Pledges To Overhaul Its Sexual Harassment Policy After Global Protests

Cisco Removed Its Seventh Backdoor Account This Year, and That's a Good Thing More | Reply Login
Cisco Removed Its Seventh Backdoor Account This Year, and That's a Good Thing

- **the number of backdoor accounts.** (Score:1)
  by Anonymous Coward
  seven down so many more to go.
  - **Re:** (Score:1)
    by Anonymous
    Password:
    Public Terminal
    Log In Forgot your password?
    Close
    Perhaps they just magically appear on their own. Someone at Cisco had to put them there. Someone at Cisco had to be told to put them there. It is impossible that Cisco didn't know these backdoors were there.
  - **Re:** (Score:1)
    by Narcocide (102829)
    Well, unlikely but not completely impossible. Of course, if they really didn't already know, that actually says something far worse about them.
    2 hidden comments
  - **Re:** (Score:1)
    by Narcocide (102829)
    Your racist ascii-art skills are garbage. What, did you auto generate those from a gif you saved in 1995 or something?
  - **Re:** (Score:2)
    by apparently (756613)
    Okay, so you posted totally hip ASCII art of Trump's stupid fucking face, so what's your point exactly?
  - **Re:** (Score:2)
    by Joce640k (829181)
    The *REAL* question is "How is it possible that Cisco doesn't know exactly who did it, when they did it, who authorized it, etc." This is trivial even on the shittiest version control system.
    THAT is incompetence at a truly epic level.
    Not if somebody's messing with the version control, impersonating other users, etc.
    Or maybe it's somebody at management level.
  - **Cisco isn't flying with the angels.** (Score:2)
    by Excelcia (906188)
    Backdoors don't just magically appear on their own. Someone at Cisco had to put them there. Someone at Cisco had to be told to put them there. It is impossible that Cisco didn't know these backdoors were there.
    Exactly. And as per Snowden's revelations [infoworld.com] years ago. Cisco was pointed to as purposefully backdooring its products at the behest of the NSA years ago, and today they are suddenly on the side of the angels because they have graciously patched out a few of them?
    Meanwhile, what has the NSA already inst
  - **Re:** (Score:2)
    by Joce640k (829181)
    It is impossible that Cisco didn't know these backdoors were there.
    You don't know that.
    Maybe the NSA is sending a continuous stream of people to apply for jobs at CISCO and put back doors into the code.
  - **Re: the number of backdoor accounts.** (Score:1)
    by Anonymous Coward
    As someone who has first hand knowledge, many of these are put there during development, by developers, on their own, and either leave them in by accident or on purpose for ease of future development and support.
    Debugging sucks, and having a hard-coded account at least makes it suck a little less.
    1 hidden comment
- **A good thing** (Score:5, Funny)
  by alvinrod (889928) on Thursday November 08, 2018 @07:15PM (#57615022)
  It's a good thing the headline pointed out that it was a good thing. I'd never be able to have figured it out for myself if I hadn't been told. Now could someone please tell me what products to consume?
  Reply to This Share
  twitter facebook linkedin
  Flag as Inappropriate
  1 hidden comment
- **Re:** (Score:2)
  by sjames (1099)
  I suppose it's good in the same sense that a serial killer pledging to murder less people this year is good news...
- **updates $100/mo per device** (Score:2)
  by Joe_Dragon (2206452)
  updates $100/mo per device
  2 hidden comments
- **good thing? pigs arse it is** (Score:2)
  by bloodhawk (813939)
  The fact they have to search for and find the backdoors after the fact means they have broken internal security coding review processes. These should never be getting to the stage where they can be found in this fashion,.
- **Re:good thing? pigs arse it is** (Score:4, Interesting)
  by jonwil (467024) on Thursday November 08, 2018 @07:41PM (#57615120)
  Any hardware manufacturer that allows backdoors to even end up in a shipping device clearly has something wrong with the way they do software development. And when they do find things like this, they need to backtrack via version control and see who allowed this crap to happen (in terms of the developer and the all the different levels of people who were supposed to review that developers code before it got out there) and give the people who allowed it to happen or should have caught it a good talking to so the people involved change the way they do things so it cant happen again.
  Then again, given what Snowden has told us, all these backdoors in all these internet connected things may well be intentional and only closed or covered up when someone not sworn to secrecy finds one...
  Reply to This Parent Share
  twitter facebook linkedin
  Flag as Inappropriate

1 hidden comment

Re: (Score:1)
by rtb61 (674572)
Now guess what the back doors were used for, hmm, corporate environment, the home of insatiably greedy psychopaths, perhaps more than just a little insider trading. The SEC rightfully should investigate with the FBI, to see who did the back dooring and how those back doors were used, insider trading by far the most profitable way to use them, especially widely distributed back doors, billions to be made. Talk about failing to disclose stuff that would have a significant impact on share value, two reasons to

Re: (Score:2)
by Joce640k (829181)
Any hardware manufacturer that allows backdoors to even end up in a shipping device clearly has something wrong with the way they do software development.
Either that, or... enemies working inside the company.

Re: (Score:2)
by postbigbang (761081)
Yep. It means a smashed QA process.
But no one will fall on their swords. More will be found. No necks hung from a yard arm, even though the backdoors are probably known.
Were they inserted at the request of intelligence agencies? We'll never know. However, this is my suspicion. There is a great hunger for such things among the spooks.

Re: (Score:2)
by Pinky's Brain (1158667)
They don't like cooperating either, so you get one backdoor per agency.

Re: (Score:2)
by Interfacer (560564)
I suspect this is not just a matter of adding admin accounts with a fixed password.
I manage a large production control system in a pharma plant. The software is from a well known vendor (in that industry) and comes with a lot of certifications. There are no hard coded user accounts, though there are privileged accounts that I know the password of because I set them up. But regardless of the fact that I know those passwords, this is an enormous pile of software comprised of services, user applications, scrip

Re: (Score:2)
by Joce640k (829181)
I suspect this is not just a matter of adding admin accounts with a fixed password.
It won't be as simple as "cat /etc/passwd", no.

And we're surprised, uh, why? (Score:3, Funny)
by NoNonAlphaCharsHere (2201864) on Thursday November 08, 2018 @07:34PM (#57615088)
So you're saying you're surprised a company named Crisco has a lot of backdoor accounts?

Reply to This Share

twitter facebook linkedin
Flag as Inappropriate
2 hidden comments

support contracts required to get updates (Score:3)
by QuesarVII (904243) on Thursday November 08, 2018 @07:36PM (#57615104)
Cisco requires you to pay for a support contract (yearly) to have access to the updates for a switch when they already charged 3x what it's worth to begin with.

I don't know how that's even legal when you have big security holes like this. The product is not fit for use, yet you have to pay even more $ to make it "safe" again.

Reply to This Share

twitter facebook linkedin
Flag as Inappropriate
1 hidden comment

Warranty of merchantability, fitness for purpose (Score:2)
by raymorris (2726007)
The relevant legal term is "warranty of merchantability". It's an implied warranty that manufacturers cannot (successfully) disclaim. The warranty of merchantability essentially guarantees that the item is fit to sell. It doesn't guarantee the quality is better than cheaper brands, but it does warrant that the product is fit for the marketplace - that it properly suits the needs of some purchasers.
I haven't done a deep dive on these particular Cisco accounts yet since I'm off work this week. At first blus
1 hidden comment

Re: (Score:2)
by Moskit (32486)
There is a separate upgrade policy for security breaches. Cisco offered a free software upgrade for a number of such issues.
https://tools.cisco.com/securi... [cisco.com]
As a special customer service, and to improve the overall security of the Internet, Cisco may offer customers free software updates to address high-severity security problems. The decision to provide free software updates is made on a case-by-case basis. Refer to the Cisco security publication for details. Free software updates will typically be limited to Critical and High severity Cisco Security Advisories.
Sample security advisory:
https://tools.cisco.com/securi... [cisco.com]
Cisco has released free software updates that address the vulnerability described in this advisory. Customers may only install and expect support for software versions and feature sets for which they have purchased a license. They do a reasonable thing on support side by the look of it.

I beat my wife 65% less , and that's a good thing. (Score:5, Insightful)
by king neckbeard (1801738) on Thursday November 08, 2018 @07:49PM (#57615172)
Yes, the direction the code is moving in is an improvement, but that's not good, that's less awful. But the fact that there were seven backdoor accounts to remove is a huge problem.

Reply to This Share

twitter facebook linkedin
Flag as Inappropriate
1 hidden comment

Re: (Score:1)
by DNS-and-BIND (461968)
And shitty comments like this are why nobody tries to get better. Why bother if all you're going to get is abuse? It's very telling you chose a feminist way of thinking about it. They are the champions of being toxic people and granting no credit for positive developments. It's one of the reasons they lost their way some time ago.

How ridiculous (Score:1)
by enrique556 (4461637)
Does cisco hardware not run on open source software? If not, this would be a great time for open source pundits to start jumping up and down and waving their hands around.
Intel seems to have the same critical mental disability when it comes to *not* putting gaping, obvious security holes in the closed source of its firmware, so from here it's pretty obvious that even the biggest, most reputable hardware companies cannot be trusted with this task.
If I was a Cisco customer I'd be calling up my "account manage
4 hidden comments

Re: Cisco bad, Ubiquiti good (Score:1)
by CranberryKing (776846)
Yes yes. Don't read the dribble.

How many other governments had the (Score:2)
by AHuxley (892839)
keys?

Why? (Score:3)
by LaughingRadish (2694765) on Thursday November 08, 2018 @08:57PM (#57615386) Journal
Would someone care to explain how these backdoors got in the code in the first place?

Reply to This Share

twitter facebook linkedin
Flag as Inappropriate
3 hidden comments

Cisco E2500 debacle (Score:2)
by Jerry (6400)
About a couple months after I purchased a Cisco E2500 WiFi, six or seven years ago, I got had a notice pop up on my screen asking me if I wanted to update the WiFi's firmware. It explained that in order to confirm the update I had to go to Cisco's cloud server and create an account. THEN, they would update the WiFi firmware. A search around the web at the time revealed that many folks who bought Cisco WiFi's received that notice and requirement. Some suggested that the NSA forced Cisco to update their

- **How many new backdoors did they create though? (Score:2)**
  by ayesnymous (3665205)
  Otherwise they'd be in breach of their agreements they have with the government.
- **Seven Accounts? (Score:2)**
  by Weirsbaski (585954)
  Cisco removed seven backdoor accounts, huh? How many more are in there?

  That's not rhetorical- I'd really like to know.

Related Links **Top of the: day, week, month.**

- 510 comments DOJ: Strong Encryption That We Don't Have Access To Is 'Unreasonable'
- 477 comments Recruiters Are Still Complaining About No-Shows At Interviews
- 445 comments Should Developers Abandon Agile?
- 441 comments Hackers Who Attended Black Hat and DefCon Conferences Say Hotel Security Personnel Demanded Access To Their Rooms
- 416 comments 'Kernel Memory Leaking' Intel Processor Design Flaw Forces Linux, Windows Redesign

next

Google Pledges To Overhaul Its Sexual Harassment Policy After Global Protests
88 comments
previous

Vulnerability Could Make DJI Drones a Spy In the Sky
11 comments

Slashdot

Post

Get more comments

72 of 72 loaded
Submit Story
"No, no, I don't mind being called the smartest man in the world. I just wish it wasn't this one." -- Adrian Veidt/Ozymandias, WATCHMEN
FAQ
Story Archive
Hall of Fame
Advertising
Terms
Privacy Statement
Privacy Choices
Opt-out Choices
About
Feedback
Mobile View
Blog

Close

Slashdot

Working...