Introducing Netgate Nexus: Multi-Instance Management at Your Fingertips.

Terrapin SSH Attack

General pfSense Questions | 33 posts | 16 posters | 55.8k views | 21 watching | Log in to reply



jimp REBEL ALLIANCE DEVELOPER NETGATE — Dec 18, 2023, 7:55 PM

This is pretty fresh so still fairly preliminary information available at the moment: https://terrapin-attack.com/

Barrier to exploit is pretty high. Requires an MitM and certain combinations of options, namely, ChaCha20-Poly1305 and MACs which use Encrypt-then-MAC (`-etm`). The SSH daemon on pfSense does enable that combination of algorithms but (a) admins shouldn't be exposing their SSH ports to the Internet and (b) if someone can MitM your local network you probably have more pressing concerns than SSH on the firewall.

That said, if you *do* expose your SSH daemon to untrusted networks and want to work around this vulnerability, you can take one of the following actions:

1. Disable both in sshd (Recommended) -- terrapin-no-etm-no-chacha.patch
2. Disable ChaCha20-Poly1305 in sshd (MAY be sufficient) -- terrapin-no-chacha.patch

Choose **one** of those options and add the patch to the System Patches package.

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

Reject Accept

Learn more and customize

y SSH clients can still connect. If they try a different patch. Also consider ation to ensure it has encryption and he server.

algorithms on a given server:

oly1305@openssh.com in the encryption -etm in the name.

s to work ar to work bot

1 out of 33

support it. For the time being it seems like it would be more effective to disable the problematic combination of options on the server, hence these patches.

However, since it's not yet clear which method is ideal (and that may vary by environment and clients), we are not issuing a specific recommended patch until we have more information.

EDIT: Re-ordered patches to note which is recommended, removed ETM only patch.

EDIT 2: The patch to disable ChaCha and ETM is now available in System Patches Package v2.2.9 as a recommended patch. Read the linked thread before updating the package.

Remember: Upvote with the 👍 button for any user/post you find to be helpful, informative, or deserving of recognition!

Need help fast? Netgate Global Support!

Do not Chat/PM for help!

3 Replies Last reply Dec 18, 2023, 8:41 PM

16

jimp pinned this topic on Dec 18, 2023, 7:55 PM

johnpoz LAYER 8 GLOBAL MODERATOR @jimp Dec 18, 2023, 8:41 PM

@jimp The way I am reading this - if was open to this would be seeing -etm listed with the nmap script?

> *and will have MAC algorithms in the list which contain -etm in the name.*

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

nessing with the sshd conf, maybe I did

```
53
 14:36 Central Standard Time
```

1 out of 33

```
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
```

edit:
DOH!!! it is there - nevermind, going to patch it now... I can't read it seems, was looking for it at the end... ugghhh

```
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       umac-128-etm@openssh.com
```

edit2: after etm patch applied

```
$ nmap --script ssh2-enum-algos -sV -p 22 192.168.9.253
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-18 14:47 Central Standard Time
Nmap scan report for sg4860.home.arpa (192.168.9.253)
Host is up (0.0010s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.4 (protocol 2.0)
| ssh2-enum-algos:
|   kex_algorithms: (2)
|       curve25519-sha256@libssh.org
|       diffie-hellman-group-exchange-sha256
|   server_host_key_algorithms: (3)
|       rsa-sha2-512
|       rsa-sha2-256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
```

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

hanks!

ols

2

Dec 19, 2023, 12:02 AM

ying here to let you know that a
lgorithms, to be disabled. If you only
ploitable if enabled.

1 out of 33

2 Replies Last reply Dec 19, 2023, 12:40 AM

4



dennypage @Skrillor Dec 19, 2023, 12:40 AM

@Skrillor said in Terrapin SSH Attack:

> *Just replying here to let you know that a workaround requires both, ChaCha20-Poly1305 and -etm MAC algorithms, to be disabled. If you only disable one of them (patch 1 and 2), the other one may still be exploitable if enabled.*

On my firewall, results from the published vulnerability scanner seem to indicate that disabling chacha alone (patch 1) is sufficient. Are there other potential mitigating factors?

2 Replies Last reply Dec 19, 2023, 12:43 AM

0



johnpoz LAYER 8 GLOBAL MODERATOR @dennypage Dec 19, 2023, 12:43 AM

@dennypage had you disabled etm? when you disabled chacha..

I just ran the scanner against pfsense, where I ran the etm patch, but still says vuln since I did not disable chacha

```
Remote Banner: SSH-2.0-OpenSSH_9.4
```

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

ssh to the public, and there is nobody
esting attack.

lable in openssh 9.6.. But its not yet
d out a new beta even.. But looks like

ols

1 out of 33

1 Reply Last reply Dec 19, 2023, 12:47 AM

0

Skrillor @dennypage Dec 19, 2023, 12:46 AM

@dennypage said in Terrapin SSH Attack:

> *On my firewall, results from the published vulnerability scanner seem to indicate that disabling chacha alone (patch 1) is sufficient. Are there other potential mitigating factors?*

To exploit the Encrypt-then-MAC variant in practice, we additionally require a CBC cipher to be negotiated. If your implementation does not offer any -cbc cipher alongside an -etm@openssh.com MAC, the vulnerability scanner returns false for CBC-EtM. If CBC-EtM isn't supported at all, disabling chacha20-poly1305@openssh.com on its own will have the same effect.

0

dennypage @johnpoz Dec 19, 2023, 12:47 AM

@johnpoz said in Terrapin SSH Attack:

> *had you disabled etm? when you disabled chacha..*

No. I only have -etm MACs enabled. I have other things disabled (RSA), which is why I asked about other mitigating factors.

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

0

Dec 19, 2023, 12:54 AM

for ssh:

```
00000000 -0800
00000000 -0800

-0800
```

1 out of 33

```
@@ -70,7 +70,7 @@
 /* Include default configuration for pfSense */
 /* Taken from https://stribika.github.io/2015/01/04/secure-secure-shell.html */
 $sshconf = "# This file is automatically generated at startup\n";
-$sshconf .= "KexAlgorithms curve25519-sha256@libssh.org,diffie-hellman-group-exchange-
```

And the slight adjustment I made for Terrapin:

```
--- /etc/inc/globals.inc.org    2023-02-02 08:47:26.000000000 -0800
+++ /etc/inc/globals.inc        2023-02-02 22:53:00.000000000 -0800
@@ -365,7 +365,6 @@

 global $ssh_keys;
 $ssh_keys = [
-       ['type' => 'rsa', 'suffix' => 'rsa_'],
        ['type' => 'ed25519', 'suffix' => 'ed25519_'],
 ];

--- /etc/sshd.org       2023-02-02 08:47:26.000000000 -0800
+++ /etc/sshd   2023-02-02 22:53:00.000000000 -0800
@@ -70,7 +70,7 @@
 /* Include default configuration for pfSense */
 /* Taken from https://stribika.github.io/2015/01/04/secure-secure-shell.html */
 $sshconf = "# This file is automatically generated at startup\n";
-$sshconf .= "KexAlgorithms curve25519-sha256@libssh.org,diffie-hellman-group-exchange-
+$sshconf .= "KexAlgorithms curve25519-sha256@libssh.org,curve25519-sha256\n";
```

0

dennypage @dennypage Dec 19, 2023, 4:23 AM

ning for Terrapin.

0

Dec 19, 2023, 1:58 PM

eplying here to let you know that a
C algorithms, to be disabled. If you
till be exploitable if enabled.

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

Curious, the web site says AES-GCM is not affected, and CTR algorithms are not affected in real-world scenarios. By disabling only ChaCha, the only algorithms left active in the configuration on pfSense software are AES-GCM and CTR-based options. Perhaps the web site needs an update to reflect that? Or the patch could only leave AES-GCM enabled. If there is no real-world scenario where CTR+ETM is exploitable it's questionable to label it vulnerable, but that's open for debate I suppose.

Remember: Upvote with the 👍 button for any user/post you find to be helpful, informative, or deserving of recognition!

Need help fast? Netgate Global Support!

Do not Chat/PM for help!

👍 2



dennypage @jimp Dec 19, 2023, 4:17 PM

FWIW, In addition to pfSense, I've tested a few other Linux and Mac systems using both the Terrapin scanner and ssh-audit. On those systems, even without any other changes, both scanners indicate that disabling ChaCha alone (patch 1) is sufficient. I have not tested with just disabling -etm MACs (patch 2).

Of course, both scanners could be broken...

👍 0

S

sandie Dec 19, 2023, 11:26 PM

I fully agree with everything what Jim written, but… ;) OpenSSH 9.6 anytime soon in pfSense? (23.09.2?) :)

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

👍 0

Dec 20, 2023, 1:38 PM

H 9.6 anytime soon in pfSense?

ally given the timing. Given the high
now unless new information comes up

l, informative, or deserving of recognition!

1 out of 33

Need help fast? Netgate Global Support!

Do not Chat/PM for help!

3



johnpoz LAYER 8 GLOBAL MODERATOR @jimp Dec 20, 2023, 2:18 PM

@jimp So will 9.6 be coming with the next normal release? I mean 9.5 was out a month before 23.09 dropped. I not sure why when 23.09 or even 23.09.1 came out why openssh wasn't updated to 9.5?

An intelligent man is sometimes forced to be drunk to spend time with his fools
If you get confused: Listen to the Music Play
*Please **don't Chat/PM me** for help, unless mod related*
SG-4860 26.07 | Lab VMs 2.9.0, 26.07

0

S 2 Replies Last reply Dec 20, 2023, 3:12 PM

S

sandie @johnpoz Dec 20, 2023, 3:12 PM

@johnpoz Newer <> Better often. I am going to apply Jim's patch, but we will upgrade each and every system which offers OpenSSH 9.6 (hopefully not having too many of nodes).
I was just crosschecking what is the plan. I think this problem may be urgent only for people who need to use those ciphers, but we are going to stop using them.

0

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

Dec 20, 2023, 3:14 PM

SH to the internet.

3

Dec 20, 2023, 4:01 PM

ean 9.5 was out a month before
me out why

> *to 9.5?*

We follow FreeBSD's lead here. We take whichever version is in base. At the moment that is 9.5p1 on dev snapshots. If they put 9.6 in base and we merge after that point, we'll pick it up.

Remember: Upvote with the 👍 button for any user/post you find to be helpful, informative, or deserving of recognition!

Need help fast? Netgate Global Support!

Do not Chat/PM for help!

👍 3



the other Dec 20, 2023, 4:50 PM

hey there,
first...thank you for your work, explanations, patch and work. :)
Then just a short feedback: although I do not have ssh open to the Internet, I used the nmap script to check..., of course, there it was: chacha and etm just as @johnpoz posted. And then it bugged me so much I installed the patch (first one of the two posted by @jimp) anyways. Rebooted, waited, checked ssh (which is still working) and got that mild feeling of relief (even though no ssh to Internet and only homenetwork with chance for MitM relatively small...but it feels better). So thanx for that one moment of easyness in pre-xmas-stress mode. :)

the other

pure amateur home user, no business or professional background
please excuse poor english skills and typpoz :)

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

👍 0

Dec 20, 2023, 7:12 PM

n Patches Package v2.2.9 as a
package.

ul, informative, or deserving of recognition!

michmoor LAYER 8 REBEL ALLIANCE @jimp Dec 21, 2023, 3:51 AM

@jimp

The patch works out nicely. Thanks to the prompt response.

🔒 Log in to view 🔒 Log in to view

Firewall: NetGate,Palo Alto-VM,Juniper SRX
Routing: Juniper, Arista, Cisco
Switching: Juniper, Arista, Cisco
Wireless: Unifi, Aruba IAP
JNCIP,CCNP Enterprise

👍 0

johnpoz referenced this topic on Dec 27, 2023, 11:54 AM

monsen Jan 3, 2024, 3:03 AM

I just noticed that this patch seems to "break" shh connectivity with Windows.

After applying the patch (and restarting the ssh deamon), when trying to SSH to the box from Windows, it now just reports

```
Corrupted MAC on input.
ssh_dispatch_run_fatal: Connection to 10.11.11.1 port 22: message authentication code i
```

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

in. I made sure to test from multiple
blem.

use "umac-128@openssh.com" as the
ed on the pfsense box after the patch. It
Windows_8.6p1, LibreSSL 3.4.3; among

he umac-128@openssh.com algorithm
g Windows to use AES-GCM.

sed by the patch, it is still present even
algorithms it would have picked then, I
nically what will trigger the "bad" MAC

ent version compiled for Windows),

1 out of 33

(Running Netgate 4100, 23.09.1-RELEASE)

2



STLJonny @monsen Jan 7, 2024, 12:52 AM

@monsen

Simple fix that I've found, to fix my Windows to be able to ssh to my pfSense install (after applying the patch) is the following.

Add the following like to c:\users<user>.ssh/config

MACs hmac-sha2-512

This forced my ssh to use that MAC (message authentication code), of which pfSense is fine with.

2

11 days later



JonathanLee Jan 17, 2024, 3:47 PM

So is cha cha poly safe to use at this point? That is supposed to be the new advanced encryption algorithm. Disabling it kind of lets the bad guys win as we are degrading our systems by way of encryption algorithms. Is there a solution. Yes I am also aware that OpenVPN side doesn't have support for it yet. The SMID assembly code is available on the processor I am using. Is this a software issue

eeding edge software issues?

Based on the vulnerability explanation it

ility? That exploit seems to have the

a better suited to this attack when they

0

Feb 21, 2024, 5:20 PM

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.



stephenw10 NETGATE ADMINISTRATOR @jimp Feb 21, 2024, 5:26 PM

@jimp said in Terrapin SSH Attack:

> *After applying the patch, reboot or restart the SSH daemon:*
>
> ## */usr/local/bin/php-cgi -f /etc/sshd*

Like that. ^

👍 0

2 months later

D

DominikHoffmann Apr 24, 2024, 5:10 PM

I take it, pfSense 24.03 has fixed this. Am I correct?

👍 0

netgate Apr 24, 2024, 7:53 PM

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

👍 1

Aug 30, 2024, 12:46 PM

Does one manually have to upgrade

0



stephenw10 NETGATE ADMINISTRATOR Aug 30, 2024, 12:52 PM

There is a patch in the system patches package to disable the affected ciphers. Apply it.

0

4 months later

W

willowen100 Dec 23, 2024, 8:56 PM

Hi

I know this is an old post, I'd like to add that I too am having problems connecting from a Windows client PC using OpenSSH.

With the below patch applied
Workaround for Terrapin SSH Attack (After applying the patch, reboot or restart the SSH daemon, FreeBSD-SA-23:19.openssh, Terrapin Attack)

I get an error connecting

```
PS C:\Users\Will> ssh admin@192.168.5.1
Corrupted MAC on input.
```

t 22: message authentication code

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

```
umac-64-etm@openssh.com
```

If I try connecting with the first MAC algorithm I get a prompt to try different ones

```
PS C:\Users\Will> ssh admin@192.168.5.1 -m hmac-sha1
Unable to negotiate with 192.168.5.1 port 22: no matching MAC found. Their offer: hmac-
```

The only way to connect to pfSense via SSH is with

```
ssh admin@192.168.5.1 -m hmac-sha2-512
```

Once in pfSense I'm able to get the OpenSSH version

```
[2.7.2-RELEASE][admin@pfSense.lan]/root: ssh -V
OpenSSH_9.4p1, OpenSSL 3.0.12 24 Oct 2023
```

Some more information can be found here at the link below
https://serverfault.com/questions/994646/ssh-on-windows-corrupted-mac-on-input

Is there any fix with this on the pfSense CE edition?

👍 0



STLJonny @willowen100 Dec 23, 2024, 11:21 PM

@willowen100 See my reply, above in this thread, for a fix from the windows side.

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

👍 1

Dec 24, 2024, 9:09 AM

👍 0

Dec 24, 2024, 3:48 PM

to utilize that encryption algorithm.

I'd have rather found a more elegant workaround (preferably on the pfSense side, so the mod only has to be done in one location), but this works in a pinch.

0

M marcosm unpinned this topic on May 1, 2026, 2:27 PM

Copyright 2026 Rubicon Communications LLC (Netgate). All rights reserved.
Privacy Policy · Cookie Policy

netgate

We (Netgate) and selected third parties collect personal information as specified in the privacy policy and use cookies or similar technologies for technical purposes and, with your consent, for **functionality, experience, measurement and "marketing (personalized ads)"** as specified in the cookie policy.
You can freely give, deny, or withdraw your consent at any time by accessing the preferences panel. Denying consent may make related features unavailable.
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.