Bug 1883988 (CVE-2020-25645) - CVE-2020-25645 kernel: Geneve/IPsec traffic may be unencrypted between two Geneve endpoints

Keywords: Security ×

Status: CLOSED ERRATA
Alias: CVE-2020-25645
Product: Security Response
Component: vulnerability
Version: unspecified
Hardware: All
OS: Linux
Priority: medium
Severity: medium
Target Milestone: ---
Assignee: Red Hat Product Security
QA Contact:
Docs Contact:
URL:
Whiteboard:
Depends On: 1885994 1884481 1885144 1885145 1885146 1885147 1885148 ~~1886425~~
Blocks: 1879667
TreeView+ depends on / blocked

Reported: 2020-09-30 16:51 UTC by Guilherme de Almeida Suckevicz
Modified: 2021-03-16 19:18 UTC (History)
CC List: 50 users (show)
Fixed In Version: Linux kernel 5.9-rc7
Doc Type: If docs needed, set a value
Doc Text: A flaw was found in the Linux kernel. Traffic between two Geneve endpoints may be unencrypted when IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel allowing anyone in between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.
Clone Of:
Environment:
Last Closed: 2021-03-16 19:18:58 UTC

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2021:0856	0	None	None	None	2021-03-16 13:51:03 UTC
Red Hat Product Errata	RHSA-2021:0857	0	None	None	None	2021-03-16 13:51:58 UTC

Guilherme de Almeida Suckevicz 2020-09-30 16:51:25 UTC — Description

A flaw was found in the Linux kernel's implementation of GENEVE tunnels combined with IPsec. The traffic between two Geneve endpoints may be unencrypted when IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel. This would allow anyone in between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.

Reference and upstream patch:
https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=34beb21594519ce64a55a498c2fe7d567bc1ca20

Alex 2020-10-06 10:58:01 UTC — Comment 8

Mitigation:

A possible workaround for this flaw is to configure IPsec for all traffic between the endpoints, instead of specifically for the UDP port used by the GENEVE tunnels. If GENEVE tunnels are not used, this flaw will not be triggered. In that case, it is possible to disable those tunnels, by unloading the "geneve" kernel module and blacklisting it (See https://access.redhat.com/solutions/41278 for a guide on how to blacklist modules).

Alex 2020-10-06 11:01:38 UTC — Comment 9

More detailed description (and keeping comment 0 short description too):

A flaw was found in the Linux kernel's implementation of GENEVE tunnels combined with IPsec. When IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel, the kernel isn't correctly routing tunneled data over the encrypted link, and sending the data unencrypted instead. This would allow anyone in between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.

Petr Matousek 2020-10-08 12:29:17 UTC — Comment 12

Acknowledgments:

Name: Mark Gray (Red Hat), Sabrina Dubroca (Red Hat)

Petr Matousek 2020-10-08 12:29:58 UTC — Comment 13

Created kernel tracking bugs for this issue:

Affects: fedora-all [~~bug 1886425~~]

Justin M. Forbes 2020-10-08 18:46:04 UTC — Comment 14

This was resolved for Fedora with the 5.8.12 stable kernel updates.

errata-xmlrpc 2021-03-16 13:50:59 UTC — Comment 18

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7

Via RHSA-2021:0856 https://access.redhat.com/errata/RHSA-2021:0856

errata-xmlrpc 2021-03-16 13:51:56 UTC Comment 19

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7

Via RHSA-2021:0857 https://access.redhat.com/errata/RHSA-2021:0857

Product Security DevOps Team 2021-03-16 19:18:58 UTC Comment 20

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

https://access.redhat.com/security/cve/cve-2020-25645