Product Support Notice

PSN # PSN004039u

Original publication date: 25-Jul-13. This is Issue #01, published date: 25-Jul-13.

Severity/risk level Medium Urgency When convenient

Name of problem Avaya VPN Gateway Node/Cluster May Restart Due to Underlying Kernel BUG in inode.c:1157 Condition

Products affected

Avaya VPN Gateway – all versions

Problem description

The Avaya VPN Gateway software platform operates on a third-party hardened Linux 2.4-based kernel. Reports from the field have identified an unresolvable condition that may unexpectedly and without prior warning affect normal system operation. Such an impact may require manual restart of the affected node or nodes within a cluster.

Log review via root console access is required to verify if the following condition has been met. Kernel crashes are logged to the system console and captured in the /var/log/messages.x (messages.1, messages.2) files.

Feb 1 11:13:09 a10-147-128-5 kernel: ------------[cut here]------------
Feb 1 11:13:09 a10-147-128-5 kernel: kernel BUG at inode.c:1157!
Feb 1 11:13:09 a10-147-128-5 kernel: invalid operand: 0000
Feb 1 11:13:09 a10-147-128-5 kernel: CPU: 2
Feb 1 11:13:09 a10-147-128-5 kernel: EIP: 0010:[iput+248/560] Tainted: P
Feb 1 11:13:09 a10-147-128-5 kernel: EIP: 0010:[<c015c0e8>] Tainted: P
Feb 1 11:13:09 a10-147-128-5 kernel: EFLAGS: 00010287[i]
Feb 1 11:13:09 a10-147-128-5 kernel:
Feb 1 11:13:09 a10-147-128-5 kernel: EIP is at (2.4.20-28.7custom)
Feb 1 11:13:09 a10-147-128-5 kernel: eax: ffffff00 ebx: da24e100 ecx: 00000020 edx: f7606b80
Feb 1 11:13:09 a10-147-128-5 kernel: esi: da24e100 edi: 00000000 ebp: d8631f28 esp: d8631f1c
Feb 1 11:13:09 a10-147-128-5 kernel: ds: 0018 es: 0018 ss: 0018
Feb 1 11:13:09 a10-147-128-5 kernel: Process sh (pid: 32311, stackpage=d8631000)
Feb 1 11:13:09 a10-147-128-5 kernel: Stack: d8640e80 da24e100 da24e100 d8631f4c c015911a da24e100 d8631f70 d8631f78
Feb 1 11:13:09 a10-147-128-5 kernel: f89ac141 f89ac0b8 d879df80 f7bccf00 d8631f78 c014622c d8640e80 d8640e80
Feb 1 11:13:09 a10-147-128-5 kernel: ec36c048 312e3237 f7b88b80 d8640e80 f4c35980 d879df80 00000000 d8631f9c
Feb 1 11:13:09 a10-147-128-5 kernel: Call Trace: [dput+250/368] (0xd8631f2c))
Feb 1 11:13:09 a10-147-128-5 kernel: Call Trace: [<c015911a>] (0xd8631f2c))
Feb 1 11:13:09 a10-147-128-5 kernel: [8021q:__insmod_8021q_O/lib/modules/2.4.20-28.7custom/kernel/net/8+-1527487/96] (0xd8631f3c))
Feb 1 11:13:09 a10-147-128-5 kernel: [<f89ac141>] (0xd8631f3c))
Feb 1 11:13:09 a10-147-128-5 kernel: [8021q:__insmod_8021q_O/lib/modules/2.4.20-28.7custom/kernel/net/8+-1527624/96] (0xd8631f40))
Feb 1 11:13:09 a10-147-128-5 kernel: [<f89ac0b8>] (0xd8631f40))
Feb 1 11:13:09 a10-147-128-5 kernel: [fput+220/256] (0xd8631f50))
Feb 1 11:13:09 a10-147-128-5 kernel: [<c014622c>] (0xd8631f50))
Feb 1 11:13:09 a10-147-128-5 kernel: [filp_close+146/160] (0xd8631f7c))
Feb 1 11:13:09 a10-147-128-5 kernel: [<c0144d12>] (0xd8631f7c))
Feb 1 11:13:09 a10-147-128-5 kernel: [sys_dup2+180/240] (0xd8631fa0))
Feb 1 11:13:09 a10-147-128-5 kernel: [<c0153de4>] (0xd8631fa0))
Feb 1 11:13:09 a10-147-128-5 kernel: [system_call+51/56] (0xd8631fc0))
Feb 1 11:13:09 a10-147-128-5 kernel: [<c0108e53>] (0xd8631fc0))
Feb 1 11:13:09 a10-147-128-5 kernel:
Feb 1 11:13:09 a10-147-128-5 kernel:
Feb 1 11:13:09 a10-147-128-5 kernel: Code: 0f 0b 85 04 b4 e4 27 c0 e9 15 01 00 00 8b 16 39 f2 0f 84 be
Feb 1 11:13:09 a10-147-128-5 kernel: <0>Kernel panic: BUG

Resolution

Root cause or trigger point for this condition has not been identified and no solution is available for the underlying Linux 2.4-based kernel platform.

Workaround or alternative remediation

Should an individual or cluster node experience this issue, Avaya recommends a cold start power cycle of affected equipment to restore system service.

Remarks

This issue has been detailed in KCS SOLN226576 VPN Gateway - System Restart Due to Kernel Panic "kernel BUG at inode.c:1157!"

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

n/a

Download

n/a

Patch install instructions | Service-interrupting?

n/a | No

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

n/a

Avaya Security Vulnerability Classification

Not Susceptible

Mitigation

n/a

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.