TECHNICAL NOTE

Vidyo Server Security Update 19 for VidyoGateway™

Document Version A

www.vidyo.com
1.866.99.VIDYO

Vidyo Server Security Update 19

Vidyo Server Security Update 19 provides existing VidyoGateway servers with updated packages and package configurations to address most known and current vulnerabilities (CVEs) at the time of the release of this Update, as noted in common OS and package security bulletins.

The updates and configuration changes applied by SU19 are outlined in System Changes Performed by Security Update 19.

Note If you have an on-premises VidyoGateway, all the information in this Technical Note applies to you. In particular, you must follow the steps in the Applying Security Update 19 section in order to physically perform the update.

If you are a cloud customer, Vidyo will install SU19 for you; however, you may want to read this Technical Note to understand the system changes that take place when SU19 is applied.

Important Notices

- This update is applicable to all maintained Vidyo servers. For more information, please refer to the Vidyo Software Maintenance Policy.
- In accordance with the *Vidyo End of Life Process Announcement for Vidyo Server Components Based on ASUS and Supermicro Platforms*, these platforms are no longer under software maintenance. Therefore, if you have these platforms, upgrading to Security Update 19 will be blocked.

Security Update 19 Files

This SU19 file…	Is for…
Security_Update-SU19-VG-bundle-v1072.vidyo	■ VidyoGateway version 3.5.2

Note Do not install SU19 on a version earlier than the versions listed in the preceding table. If SU19 is run on an unsupported version, the updater will exit and post a message in the updater log.

System Changes Performed by Security Update 19

Specific security-related package updates:

- Java

Product	SU18 Version	SU19 Version
VidyoGateway	JRE 1.8 Update 171	JRE 1.8 Update 181

- Apache Web Server

Product	SU18 Version	SU19 Version
VidyoGateway	2.4.33 with OpenSSL 1.0.2o	2.4.34 with OpenSSL 1.0.2o

Note This SU updates the configuration to use the random Diffie-Hellman parameters file (2048 bits).

- Apache Tomcat

Product	SU18 Version	SU19 Version
VidyoGateway	8.0.51	8.5.32

- OpenSSL Dynamic Library

Product	SU18 Version	SU19 Version
VidyoGateway	OpenSSL 1.0.2o	OpenSSL 1.0.2o

- Wget

Product	SU18 Version	SU19 Version
VidyoGateway	1.19.2 (OpenSSL 1.0.2o)	1.19.2 (OpenSSL 1.0.2o)

- OpenSSH

Product	SU18 Version	SU19 Version
VidyoGateway	7.6p1 (OpenSSL 1.0.2o)	7.6p1 (OpenSSL 1.0.2o)

OpenSSH Security Improvements

- Devices are now configured to time out after 60 seconds for incomplete or broken SSH sessions by setting LoginGraceTime to 60 seconds.
- Addresses a security scan issue “Diffie-Hellman group smaller than 2048 bits (tls-dh-prime-under-2048-bits)” by removing groups lower than 2048 bits from /etc/ssh/moduli.
- Adds the following cipher, HMAC, and exchange algorithm lines to the sshd_config.default to strengthen SSH encryption:
  - aes128-ctr,aes192-ctr,aes256-ctr
  - hmac-sha2-256,hmac-sha2-512
  - ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256

These improvements require an SSH client that supports the above listed ciphers, HMACs, and key exchange algorithms. SSH clients that do not support these mechanisms will not be able to connect. Most modern updated SSH clients usually support these mechanisms.

Linux® Kernel Update

- SU19 will update the Linux Kernel to 4.14.58

Known Issues after Successfully Applying Security Update 19

Some vulnerability scanners may report a low to moderate level vulnerability of “TCP timestamp response (generic-tcp-timestamp)” and/or “ICMP timestamp response”, even after Security Update 19 is successfully applied.

Description: The remote host responded with a TCP timestamp. The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP timestamps. At this time, Vidyo is reluctant to disable tcp_timestamps, as this could disrupt the packet communication needs of the protocols used for VidyoConferencing. Vidyo considers this vulnerability to be low, and this issue does not really affect the security of the Linux TCP stack in any meaningful way. ICMP may be blocked via a firewall to mitigate the ICMP specific tcp_timestamp issue.

Applying Security Update 19

If you have an on-premises VidyoGateway, you must perform the steps in this section to apply SU19. If you are a cloud customer, you can skip this section because Vidyo will perform the update for you.

VidyoGateway

1. Log in to the *VidyoGateway Configuration* page: **`http://{Gateway IP or FQDN}`**.
2. Click the **Upgrade Gateway** link.
3. Click **Browse**.
4. Select and open the Security_Update-SU19-VG-bundle-v1072.vidyofile.
5. Click **Upload and Install** on the *Upgrade Gateway* page.

   The system will reboot after uploading the update package.

Note The update process can take several minutes (allow 5 to 10 minutes for the process to complete once the server has stated it is restarting). You will not be able to access the system via the browser during the update process. After 15 minutes, you may manually refresh your browser to again access to the VidyoGateway.

   A copy of the Updater log will be available for review. For more information, see Updater Log.

6. Review the log to ensure the update completed successfully.

   A completed message will be noted near the end of the log file. If the log states the update did not complete or logged errors, review the log for the reason and address it as needed.

7. See Contacting Technical Support for more information about getting assistance.
8. Repeat steps 1 through 6 for each VidyoGateway with the system.
9. Test that each VidyoGateway is functional.

Contacting Technical Support

If you are a Vidyo Reseller or Vidyo End User with “Plus” coverage, please feel free to contact the Vidyo Customer Support team via email with any questions or if you need assistance.

- Phone: +1-866-99-VIDYO / +1-201-289-8597
- Email: support@vidyo.com

If you are a Vidyo End User without “Plus” coverage, please contact your Vidyo Reseller for further details.