TECHNICAL NOTE

Vidyo Server Security Update 18 for VidyoPortal™ , VidyoRouter™, and VidyoGateway™

www.vidyo.com
1.866.99.VIDYO

Vidyo Server Security Update 18

Vidyo Server Security Update 18 provides existing Vidyo servers (VidyoPortals, VidyoRouters, and VidyoGateways) 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 SU18 are outlined in System Changes Performed by Security Update 18.

Note If you have an on-premise VidyoPortal and/or VidyoRouter, all the information in this Technical Note applies to you. In particular, you must follow the steps in the Applying Security Update section in order to physically perform the update.

If you are a cloud customer, Vidyo will install SU18 for you; however, you may want to read this Technical Note to understand the system changes that take place when SU18 is applied.

Important Notices

- If you have an on-premise VidyoPortal, before applying SU18, Vidyo highly recommends that you back up your database and then download the backup to your local machine.
- 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 18 will be blocked.

Security Update 18 Files

This SU18 file…	Is for…
Security_Update18-Rev009-G2signed.vidyo	■ VidyoPortal version 18.1.0 or later (with SU17)
Security_Update18-Rev009-G2signed.vidyo	■ VidyoRouter version 18.1.0 or later (with SU17)
Security_Update-SU18-VG-bundle-v763.vidyo	■ VidyoGateway version 3.5.2 or later

Note Do not install SU18 on a version earlier than the versions listed in the preceding table. If SU18 is run on an unsupported version, the updater will exit and post a message in the updater log.

Updater Log

All updater messages are logged in an updater log file created during the update. This log file is used for any subsequent updates, and each updater will append its log messages to this file. At the end of the update process, this log file is then copied to a location that users can access and download for review via each product's respective Web UI:

- **VidyoPortal**: The updater log file is copied and available for download at *Super Admin Pages* > *Settings* > *Maintenance* > *Database* as follows: **`updat_{date}_{time}_{timezone}.log`**. The file can be downloaded or deleted as needed.
- **VidyoRouter (Standalone)**: The updater log file is copied and available for download at */vr2conf pages /Logs* as follows: **`vr2.log.updates{date}_{time}_{timezone}`**. The file can only be downloaded; it cannot be deleted.

System Changes Performed by Security Update 18

Specific security-related package updates:

- Java

Product	Original Version	SU18 Version
VidyoPortal	JRE 1.8 Update 151	JRE 1.8 Update 171
VidyoRouter	JRE 1.8 Update 151	JRE 1.8 Update 171
VidyoGateway	JRE 1.8 Update 151	JRE 1.8 Update 171

- Apache Web Server

Product	Original Version	SU18 Version
VidyoPortal	2.4.29 with OpenSSL 1.0.2n	2.4.33 with OpenSSL 1.0.2o
VidyoRouter	2.4.29 with OpenSSL 1.0.2n	2.4.33 with OpenSSL 1.0.2o
VidyoGateway	2.4.29 with OpenSSL 1.0.2n	2.4.33 with OpenSSL 1.0.2o

- Apache Tomcat

Product	Original Version	SU18 Version
VidyoPortal	8.0.48	8.0.51
VidyoRouter	8.0.48	8.0.51
VidyoGateway	8.0.48	8.0.51

- OpenSSL Dynamic Library

Product	Original Version	SU18 Version
VidyoPortal	OpenSSL 1.0.2n	OpenSSL 1.0.2o
VidyoRouter	OpenSSL 1.0.2n	OpenSSL 1.0.2o
VidyoGateway	OpenSSL 1.0.2n	OpenSSL 1.0.2o

- Wget

Product	Original Version	SU18 Version
VidyoPortal	1.19.2 (OpenSSL 1.0.2n)	1.19.2 (OpenSSL 1.0.2o)
VidyoRouter	1.19.2 (OpenSSL 1.0.2n)	1.19.2 (OpenSSL 1.0.2o)
VidyoGateway	1.19.2 (OpenSSL 1.0.2n)	1.19.2 (OpenSSL 1.0.2o)

- MySQL

Product	Original Version	SU18 Version
VidyoPortal	5.6.38 Community Edition	5.6.39 Community Edition

- OpenSSH

Product	Original Version	SU18 Version
VidyoPortal	7.6p1 (OpenSSL 1.0.2n)	7.6p1 (OpenSSL 1.0.2o)
VidyoRouter	7.6p1 (OpenSSL 1.0.2n)	7.6p1 (OpenSSL 1.0.2o)
VidyoGateway	7.6p1 (OpenSSL 1.0.2n)	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

- SU18 will update the Linux Kernel to 4.14.34

Known Issues after Successfully Applying Security Update 18

- 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 18 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.

- After upgrading to Security Update 18 and rebooting the system, the wrong alert message displays stating “Applied” instead of “Applied system rebooting.”

Applying Security Update 18

If you have an on-premise VidyoPortal and VidyoRouter, you must perform the steps in this section to apply SU18. If you are a cloud customer, you can skip this section because Vidyo will perform the update for you.

VidyoPortal without Hot Standby

For VidyoPortals configured with Hot Standby, see VidyoPortal with Hot Standby.

1. Log in to the VidyoPortal Super Admin pages: **`http://{Portal IP or FQDN}/super`**.
2. Navigate to *Settings* > *Maintenance* > *Database*.
3. Click **Backup** to make a backup copy of the VidyoPortal database.
4. Select the checkbox for the newly created database backup file.
5. Click **Download** to download and save a copy of the database file.
6. Navigate to *Settings* >*Maintenance* > *Upgrade*.
7. Click **Browse…**.
8. Locate and select the appropriate **`.vidyo`** (as noted in the table on page 3) file from the file selection dialog box.
9. Click **Open**.
10. Click **Upload**.

    The system will reboot after uploading the update package.

Note The update process can take several minutes (allow 5 to 15 minutes for the process to complete once the server has stated it is restarting). Do not attempt to refresh the browser and access the server until the process is complete. You will not be able to access the system via the browser during the update process. Once the update process is completed, your browser should refresh and you will be able to browse and log in to the system again. If your browser does not refresh to the login screen automatically after 30 minutes, then manually refresh your browser.

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

11. 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.

See Contacting Technical Support for more information about getting assistance.

12. Test the VidyoPortal to ensure that it is functional.

VidyoPortal with Hot Standby

If you have a VidyoPortal configured with Hot Standby, you have two options for applying SU18:

- Option 1 provides the least amount of down time, but may cause some Call Detail Records (CDR) records to be lost. This may occur because the VidyoPortal that is Active and the VidyoPortal that is Standby are switched, causing all database and CDR changes to be lost since the last successful synchronization.
- Option 2 takes more time because you must take the system completely offline for full maintenance, but no CDR records will be lost.

Option 1

With this option, you upgrade the Standby VidyoPortal first, sync the two VidyoPortals, and then switch VidyoPortals.

If you are using VidyoPortal 3.4.4 or later, do the following:

1. Place the VidyoPortal that is currently the Standby VidyoPortal (i.e., VidyoPortal 2) into Maintenance mode.
2. Apply SU18 to the VidyoPortal that is in Maintenance mode.
3. Return the VidyoPortal to Standby mode by disabling Maintenance mode after the upgrade is complete and the server is restarted.
4. Access the Super Admin pages on the Active VidyoPortal to ensure that the databases have been synchronized successfully:
    a. Navigate to *Settings* > *Hot Standby* > *Status*.
    b. Verify that the sync has completed by ensuring the **Database Synchronization** field displays that the databases are “In Sync.”
5. Switch the VidyoPortals:
    a. Navigate to *Settings* > *Hot Standby* > *Status*.
    b. Click **Force Standby**.
    c. Click **Yes** in the *Confirmation* dialog box to force the Active VidyoPortal into Standby mode.
6. Place the previous Active VidyoPortal that is now the Standby VidyoPortal (i.e., VidyoPortal 1) into Maintenance mode after the VidyoPortals have been switched.

7. Apply SU18 to the VidyoPortal that is in Maintenance mode.
8. Return the VidyoPortal to Standby mode by disabling Maintenance mode after the upgrade is complete and the server is restarted.

Option 2

With this option, you place both servers into Maintenance mode, upgrade both, and then return them to their original Active and Standby modes.

1. Place the VidyoPortal that is currently the Standby VidyoPortal (i.e., VidyoPortal 2) into Maintenance mode.
2. Place the VidyoPortal that is currently the Active VidyoPortal (i.e., VidyoPortal 1) into Maintenance mode.
3. Return the VidyoPortal that was originally the Active VidyoPortal (i.e., VidyoPortal 1) to Active mode first after the upgrades are complete and the servers have restarted.
4. Return the VidyoPortal that was originally the Standby VidyoPortal (i.e., VidyoPortal 2) to Standby mode.

Standalone VidyoRouter

1. Log in to the Standalone VidyoRouter configuration pages: **`http://{Router IP or FQDN}/vr2conf`**.
2. Click the *Upload* tab.
3. Click **Upload and Upgrade**.
4. Locate and select the appropriate **`.vidyo`** file (as noted in the table on page 3) for 64-bit VidyoRouters (64-bit VidyoRouters will have “(64-bit)” in the Ver: name as displayed on the *Upload* page).
5. Click **OK** in the pop-up.

   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 gain access to the VidyoRouter.

   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.

See Contacting Technical Support for more information about getting assistance.

7. Repeat steps 1 through 6 for each Standalone VidyoRouter in the system.
8. Test that the VidyoPortal and each VidyoRouter is functional.

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_18_Rev009-signed.vidyo`** file.
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.