BOGEN COMMUNICATIONS LLC

Technical Service Bulletin

No. C4-2026-08

October 23, 2026

Subject: Critical PHP Security CVE-2026-109618 and CVE-2026-109619

Applicable Product: Bogen Nyquist C4000
Priority: Critical

Overview

A critical security vulnerability affecting PHP has been identified as **CVE-2026-109618 and CVE-2026-109619**. Exploitation of CVE-2026-109618 and CVE-2026-109619 does not require authentication; both vulnerabilities can be triggered remotely by an unauthenticated attacker, and the PHP Security Team assigned a CVSS v4.0 score of 9.2 (Critical). Because unauthenticated remote exploitation is possible, any Nyquist server reachable from untrusted networks - including the Internet or any network segments accessible to third parties - should be treated as high risk and remediated immediately. Customers must prioritize upgrading to a Nyquist release that includes the patched PHP package, and if an immediate upgrade is not possible you should isolate the server from untrusted networks, restrict access to the web interface to trusted management IPs or a VPN with MFA.

Because PHP is a component of the web-based user interface provided by Bogen Nyquist servers, customers should update the Debian operating system components on their Nyquist servers as soon as possible.

Important Note: The updated PHP package that resolves this issue is only available for Nyquist C4000 7.0.1.535 and C4000 11.0.0.652. There is no available fix for previous Nyquist releases; upgrading to one of the Nyquist releases listed above is strongly advised.

Note: This issue and instructions apply to Nyquist System Controllers and Custom Servers running Nyquist software. Nyquist systems running on Custom Servers should also follow these instructions.

Required Customer Action

1. On Nyquist servers running C4000 7.0.1.535 and C4000 11.0.0.652, install the latest Debian operating system component updates using the instructions provided in this technical service bulletin under the section entitled, “Upgrade Procedure”.
2. If your Nyquist server is running a C4000 release older than release 7.0, update your C4000 Nyquist server to the latest release as soon as possible.
3. If you’re not able to update the C4000 Nyquist server at this time, and if your Nyquist server is attached to the Internet for Internet based services like **Internet Radio Services**, we strongly

suggest that you remove the Internet connection from the Nyquist server or restrict access via firewall to known IP addresses until you're able to update the Nyquist server to a release that supports the security fix for this security issue. Without the security update, Nyquist should be isolated from untrusted network access. If the server must remain connected, access to the Nyquist server should be restricted through properly configured firewall rules to only known, trusted IP addresses. This mitigation should be implemented and validated by the customer's IT or network security team.

Restrict access to the Nyquist web interface to a limited set of management IP addresses via firewall rules or network ACLs.

Urgent summary: Treat these PHP vulnerabilities as **remotely exploitable without trust** and act immediately. If you cannot apply the Debian component upgrade right away, perform the following emergency steps now.

- **Isolate the server**
  - Immediately remove the Nyquist server from any untrusted networks and the public Internet if feasible.
  - If full disconnection is not possible, place the server behind a firewall that blocks all inbound access except from a small set of trusted management IPs.
- **Emergency patching and scheduling**
  - Prioritize upgrading to a Nyquist release that includes the patched PHP package (see bulletin note) as the primary remediation.
  - If you cannot upgrade immediately, schedule the upgrade for the next available maintenance window and treat it as critical.
- **Network access controls**
  - Restrict access to the Nyquist web interface to a VPN or bastion host only; require multi-factor authentication for administrative access.
  - Block or limit outbound connections from the Nyquist server to reduce risk of data exfiltration if compromised.

Before Beginning the Upgrade

1. Schedule an appropriate maintenance window. The Nyquist server will not be fully operational while Debian components are being upgraded.
2. If possible, create and export a current Nyquist system backup before beginning.
3. Verify that the Nyquist server can access the following sites:
   - deb.debian.org
   - security.debian.org
   - dl-ssl.google.com
   - bogen-ssu.bogen.com

4. Customers using Nyquist Automatic Failover should follow the applicable maintenance and server-access procedures documented in the Nyquist System Administrator Guide.

The upgrade duration can vary, and the server is not fully operational during the process.

Debian Upgrade Procedure

Perform the following steps on each Bogen Nyquist server:

1. Sign in to the Nyquist web interface using an account with administrative permissions.
2. From the navigation bar, select **System Parameters**.
3. Select **Check Internet Site Access**.
4. Verify that the required update sites report the status of **SUCCESS**.
5. Return to **System Parameters** and select **System Update**.
6. Select **Upgrade Debian Operating System Components**.
7. Review the information displayed on the screen.
8. Select **Start Upgrade**.
9. Monitor the **Debian Upgrade Status** window until the process is completed.

Warning: Do not shut down, restart, disconnect power from, or otherwise interrupt the Nyquist server while the Debian upgrade is running.

If the completion message instructs you to shut down and power-cycle the server:

1. Select **Shut Down** from the **System Parameters** page.
2. Wait until the server has completely shut down and all server lights have turned off.
3. Turn the server's power switch off.
4. Wait at least 10 seconds.
5. Turn the power switch back on.

These steps are documented in the **"Upgrade Debian Operating System Components"** section of the Nyquist System Administrator Guide.

The completed package changes can be reviewed in dpkg.log under the System section of the **System Logs** page.

Important Note: You might need to run this update twice to get the correct PHP version installed. See "After the Upgrade" for details.

BOGEN COMMUNICATIONS LLC

Technical Service Bulletin

No. C4-2026-08

Automatic Failover Systems

For Nyquist systems configured with Automatic Failover, apply the Debian component upgrade to **both the Primary and Secondary servers** after disabling the Automatic Failover feature by pressing "Disable" on both servers via **Automatic Failover** web interface page.

See section "Automatic Failover" in the Nyquist System Administrator Guide for details on setting up Automatic Failure.

After the Upgrade

After the Nyquist server has restarted:

1. Confirm that the Nyquist web interface is accessible, then,
    1. From the navigation bar, select **System Parameters**.
    2. Select **Check Server Status**
    3. Scroll down to the **Software Components** section and ensure that php is version 8.2.35 or higher. Example: php 8.2.35-1~deb12u1
       If you see a version number less than 8.2.35, run the upgrade process again.
2. Confirm that normal paging and communication functions are operating.
3. Review the Nyquist Dashboard for warnings or errors.
4. For Automatic Failover systems, reactivate Automatic Failover by going through the Automatic Failover setup process again. After setup, verify the status of both servers and confirm that database replication is operating normally.

If the Upgrade Cannot Be Completed

Contact Bogen Technical Support if any of the following occurs:

- The Debian upgrade reports an unexpected error.
- The message **"Debian upgrades disabled by Bogen Administrator"** appears.
- A required Debian or Bogen update site cannot be accessed after network and firewall settings have been verified.

- The message **"WARNING: Possible Debian upgrade issues encountered"** appears.
- The Nyquist web interface or system services do not operate normally after the server restarts.

Additional Information

The Nyquist **Upgrade Debian Operating System Components** feature updates the Linux kernel and installed Debian packages while remaining within the major Debian release supported by the installed Nyquist software. Bogen recommends using this feature whenever security corrections are released for the Debian operating system or installed packages.

For information about the PHP security release, see the PHP security announcement. [news-web.php.net]

If you have any questions related to this Service Bulletin or need help with your system, please contact Bogen's Technical Support team via the Bogen Technical Support Portal.

Sincerely,

Bogen Communications LLC