PROTECTLI
TAKE BACK YOUR NETWORK

Technical Service Bulletin TSB-2026-004

EDK II PXE Network Boot Vulnerability (CVE-2026-97631)

Issue Date	November 17, 2026
Last Updated	November 17, 2026
Version	1.0.0
Severity	MEDIUM
CVE	CVE-2026-97631 (TianoCore advisory GHSA-99cj-7hg9-mp4m)
Upstream Rating	Critical, CVSS 4.0 score 9.5 (TianoCore)
Affected Products	AMI BIOS: FW4C, V1210, V1211, V1410, V1610, VP2420, VP2430, VP2430e, VP2440, VP2440e, VP3210, VP3230, VP4600 Series, VP6600 Series coreboot: VP2410 and VP4600 Series on older releases only
Affected Firmware	AMI BIOS: all current releases for the models listed coreboot: VP2410 v1.0.15; VP4600 Series v1.0.13, v1.0.16, v1.0.17
Affected Components	EDK II UEFI PXE network boot driver (UefiPxeBcDxe)
Status	AMI BIOS: MITIGATION AVAILABLE | UNDER INVESTIGATION COREBOOT: CURRENT RELEASES NOT AFFECTED

Changelog

Version	Date	Changes
1.0.0	November 17, 2026	Initial release

Executive Summary

CVE-2026-97631 is a flaw in the UEFI network boot (PXE) driver from EDK II, the open-source code that many UEFI firmware implementations, including AMI BIOS, are built on. PXE lets a device start up by loading

what it needs from a server on the network instead of from its internal drive. During that network startup, the driver mishandles oversized network error messages, which can overwrite memory the firmware is using. At minimum this can stop the device from booting. In the worst case, an attacker who can send that message at the right moment could run their own code before the operating system and Secure Boot load. TianoCore, which maintains EDK II, rates the vulnerability Critical.

The flaw can only be triggered during a UEFI network boot. A Vault that boots from its internal drive does not run the affected code, and a Vault that has finished booting is not exposed.

AMI BIOS firmware for many Protectli models includes the affected driver. On most of these models, the BIOS setting that controls it, Network Stack, is disabled by default, so the driver does not run unless a user turns it on. On the VP3210 and VP3230, Network Stack is enabled by default. A unit with factory settings will attempt a network boot if it reaches that point in its boot order, for example when no bootable drive is found.

Current coreboot releases are not affected. The vulnerable driver is not included in the firmware. We confirmed this by checking both the firmware source and the released firmware images, not just the source code. Four older coreboot releases from 2022 for the VP2410 and VP4600 Series contain the driver and should be updated.

Customers who do not use network boot should keep Network Stack disabled, which prevents the affected driver from running. Customers who use network boot should do so only on a trusted, isolated network.

Quick Reference: What Should I Do?

Your Firmware	Status	Recommended Action
AMI BIOS: VP3210, VP3230	**Affected, network boot enabled by default**	Disable Network Stack in the BIOS unless you use network boot
AMI BIOS: FW4C, V1210, V1211, V1410, V1610, VP2420, VP2430, VP2430e, VP2440, VP2440e, VP6600 Series	**Affected, but network boot is disabled by default**	Leave Network Stack disabled unless you use network boot
AMI BIOS: VP4600 Series	**Driver present but cannot run**	No action needed
AMI BIOS: FW2B, FW4B, FW6, VP2410	**Not affected**	No action needed
coreboot: VP2410 v1.0.15	**Affected**	Update to the latest coreboot release
coreboot: VP4600 Series v1.0.13, v1.0.16, or v1.0.17	**Affected**	Update to the latest coreboot release
coreboot: any other release	**Not affected**	No action needed

If you use network boot on an affected unit, see If You Use Network Boot.

Affected Systems

AMI BIOS Firmware

Protectli reviewed AMI BIOS images across current and recent releases. Within each model, the affected driver is identical in every release from 2024 through 2026, so all current AMI BIOS releases for the models below are affected. Affected models fall into three groups based on whether the driver can run with factory default settings.

Group	Models	Network Stack Default	What This Means
Enabled by default	VP3210, VP3230	Enabled	A unit with factory settings will attempt a UEFI network boot if it reaches the network entry in its boot order
Disabled by default	FW4C, V1210, V1211, V1410, V1610, VP2420, VP2430, VP2430e, VP2440, VP2440e, VP6600 Series (VP6630, VP6650, VP6670)	Disabled	The driver runs only if a user enables Network Stack in the BIOS
Driver cannot run	VP4600 Series (VP4630, VP4650, VP4651, VP4670)	Enabled	The firmware has no UEFI driver for the built-in network ports, so the affected driver has nothing to use and cannot run

AMI BIOS firmware for the FW2B (BSW4L020), FW4B (BSW4L020), FW6 (KBRL 3.00), and VP2410 (GLK4L 4.00) does not include the UEFI network stack and is not affected.

Affected AMI BIOS Releases

The table below lists the current AMI BIOS release for each affected model. Earlier AMI BIOS releases for these models should also be treated as affected.

Model	BIOS ID	BIOS Date	Status
FW4C	MBSW0104	09/23/2024	**Disabled by default**
V1210	JPL.2LAN.S4G.PCIE.6W.013	09/28/2024	**Disabled by default**
V1211	JPL.2LAN.D8G.PCIE.6W.009	09/28/2024	**Disabled by default**
V1410	JPL.4LAN.S8GB.PCIE.6W.007B	09/24/2024	**Disabled by default**
V1610	JPL.6LAN.D16G.PCIE.007	08/13/2024	**Disabled by default**
VP2420	VP2420 V1.03	08/16/2024	**Disabled by default**

VP2430	VP2430 V1.10 (ADN4L)	12/20/2024	**Disabled by default**
VP2430e	VP2430e V1.40 (ADN4L)	05/19/2026	**Disabled by default**
VP2440	ADNX7 1.00	07/24/2025	**Disabled by default**
VP2440e	ADNX7 1.40	06/10/2026	**Disabled by default**
VP3210	ADN2L 1.00	08/07/2024	**Enabled by default**
VP3230	ADN2L 1.00	08/07/2024	**Enabled by default**
VP4630	CML6A 2.50	09/11/2024	**Driver cannot run**
VP4650	CML6A 2.50	09/11/2024	**Driver cannot run**
VP4651	CMUL6 2.50	05/19/2026	**Driver cannot run**
VP4670	CMUL6 2.20	09/11/2024	**Driver cannot run**
VP6630	ADP6L 1.80	08/05/2024	**Disabled by default**
VP6650	ADP6L 1.80	08/05/2024	**Disabled by default**
VP6670	ADP6L 1.80	08/05/2024	**Disabled by default**

coreboot Firmware

The following coreboot releases include the affected driver. All other public coreboot releases for Protectli Vaults do not.

Platform	Releases Containing the Driver	First Release Without the Driver
VP2410	v1.0.15	v1.1.0
VP4600 Series (VP4630, VP4650, VP4670)	v1.0.13, v1.0.16, v1.0.17	v1.0.18

No public coreboot release for the FW4C, V1210, V1211, V1410, V1610, VP2420, VP2430, VP2430e, VP2440, VP2440e, VP3210, VP3230, or VP6600 Series contains the driver. coreboot releases for the FW2B, FW4B, and FW6 use SeaBIOS instead of EDK II, so they cannot contain the driver.

Operating Systems

This is a firmware vulnerability that is triggered before any operating system loads. The installed OS does not change exposure, whether it is OPNsense, pfSense®, Linux, Windows, or another OS.

Technical Details

Technical Background

- **Component:** EDK II NetworkPkg, PXE Base Code driver `UefiPxeBcDxe` (file GUID `B95E9FDA-26DE-48D2-8807-1F9107AC5E3A`)
- **Defect:** During a PXE boot, the driver listens for ICMP error messages and copies each one into a fixed 504-byte field. The size checks in both the IPv4 and IPv6 handlers are incorrect, so an oversized message writes past the end of the field (CWE-120, CWE-131, CWE-787). The affected code dates back to 2010.
- **Impact:** An oversized message can hang the boot. An attacker who knows the exact firmware build can achieve code execution in the DXE phase, in ring 0, before Secure Boot or measured boot has verified anything.
- **Exposure window:** Only while the device is PXE booting over IPv4 or IPv6. No authentication is required; the attacker must deliver a unicast ICMP error message to the device's IP address during that window.
- **Scoring:** TianoCore rates it CVSS 4.0 9.5 (Critical). Red Hat and SUSE score it CVSS 3.1 8.8, treating the attacker as needing adjacent network access.
- **Upstream fix:** Merged into the EDK II master branch on October 15, 2026. At the time of the advisory, no stable EDK II release included the fix.

How Protectli Firmware Was Assessed

AMI BIOS: Each image was checked for three things: whether `UefiPxeBcDxe` is present, the factory default of the Network Stack setting that controls it, and whether the image includes a UEFI driver for the built-in network ports, which PXE needs in order to run. No AMI BIOS release reviewed includes the upstream fix.

Current coreboot releases: Current coreboot releases for Protectli Vaults do not build the EDK II network stack, so `UefiPxeBcDxe` is not present. This was verified against the build configuration of every public release and by scanning the published firmware images, each matching its published SHA-256 hash, including the latest release for every platform.

Network boot on coreboot units: The network boot option in Protectli's coreboot firmware uses iPXE, a separate network boot program that does not include the affected EDK II driver.

Older coreboot releases (2022): The four releases listed above include `UefiPxeBcDxe`. Updating to a current release removes it.

Recommended Actions

AMI BIOS Units

If you do not use network boot, make sure Network Stack is disabled in the BIOS. This is most important on the VP3210 and VP3230, where it is enabled by default. Disabling it also prevents the Vault from attempting a network boot if it cannot find a bootable drive.

The Network Stack setting is in the BIOS setup screen, typically under **Advanced > Network Stack Configuration**. Menu layout can vary between models. Contact support if you need help locating it.

coreboot Units on an Older Release

If your VP2410 or VP4600 Series unit is running one of the releases listed above, update to the latest coreboot release. This removes the driver entirely.

Firmware updates are performed using **Flashli**, Protectli's firmware update utility:

1. Download the latest Flashli script from: https://github.com/protectli-root/protectli-firmware-updater
2. Follow the instructions in the repository to update your VP2410 or VP4600 Series unit to the latest coreboot release
3. For additional guidance, see the KB article: How to Use Flashli

If You Use Network Boot

If you rely on network boot for provisioning or recovery on an affected AMI BIOS unit, keep that traffic on a trusted, isolated network segment and limit which devices can send traffic to the Vault while it boots.

Permanent Resolution

AMI BIOS: Protectli is working toward an updated AMI BIOS that includes the upstream fix. There is no release timeline yet. In the meantime, disabling Network Stack prevents the affected driver from running, so units configured this way do not need to wait for an update to be protected. This bulletin will be updated as progress is made.

coreboot: Current releases already exclude the affected driver. No further firmware change is needed.

Impact on System Operation

- **Running systems:** A Vault that has finished booting is not exposed. The flaw can only be triggered during a UEFI PXE boot
- **Booting from local storage:** Booting from the internal drive does not run the affected driver
- **Secure Boot:** Does not protect against this flaw, because the affected code runs before Secure Boot verification begins
- **CISA KEV status:** As of this bulletin's issue date, CVE-2026-97631 is not listed in CISA's Known Exploited Vulnerabilities catalog

---

Frequently Asked Questions

Q: Is my Vault at risk while it is running?

A: No. The flaw can only be triggered while a device is booting over the network with UEFI PXE. A Vault that has finished booting, or that boots from its internal drive, does not run the affected code.

Q: The CVE is rated Critical. Why is this bulletin rated Medium?

A: The Critical rating describes the worst case for any EDK II based device that network boots, such as data center servers. On Protectli units, the flaw can only be triggered during a UEFI network boot, which is disabled by default on most affected models and can be turned off on all affected AMI BIOS models. It is rated Medium rather than Low because the VP3210 and VP3230 have network boot enabled by default.

Q: If I disable Network Stack, am I protected?

A: Yes. With Network Stack disabled, the affected driver does not run. On the VP3210 and VP3230, loading BIOS defaults, or a BIOS update that resets settings, turns Network Stack back on, so check the setting after either one.

Q: My coreboot boot menu has a network boot option. Is that affected?

A: No. Network boot on Protectli coreboot firmware uses iPXE, a separate program that does not include the affected EDK II driver.

Q: Does Secure Boot protect against this?

A: No. The affected code runs before Secure Boot verifies anything. If you use Secure Boot, keep it enabled, as it still protects against other threats.

Q: Does it matter which operating system I run?

A: No. The flaw is in the firmware and is triggered before any operating system loads.

References

- TianoCore security advisory GHSA-99cj-7hg9-mp4m: https://github.com/tianocore/edk2/security/advisories/GHSA-99cj-7hg9-mp4m
- NVD entry for CVE-2026-97631: https://nvd.nist.gov/vuln/detail/CVE-2026-97631
- Dasharo: Current Dasharo releases are not affected by CVE-2026-97631: https://blog.3mdeb.com/2026/2026-10-29-dasharo-edk2-pxe-cve-2026-97631/

Support and Contact Information

If you have questions about this vulnerability or need help checking or updating your firmware:

- **Email Support:** support@protectli.com
- **Support Portal:** Open a ticket through your Protectli account
- **Additional Contact Options:** https://protectli.com/contact/

Document Information

TSB Number	TSB-2026-004

Issue Date	November 17, 2026
Last Updated	November 17, 2026
Version	1.0.0

© 2026 Protectli. All rights reserved. This document may be reproduced and distributed for customer support purposes.