VIAVI Solutions Inc.
1445 South Spectrum Boulevard, Suite 102
Chandler, AZ 85286
United States
www.ViaviSolutions.com

To: Whom it may concern
Date as of: 26 October, 2026
Subject: PHP Vulnerability Assessment Update

Dear Customer,

VIAVI is aware of the recently disclosed critical PHP vulnerabilities, identified as CVE-2026-109618 and CVE-2026-109619 (commonly referred to as "PHP2Shell"). These vulnerabilities may allow remote code execution in affected PHP environments and have prompted a broad industry-wide review of products and systems that utilize PHP.

The security of our customers' networks and systems remains a top priority for VIAVI. Following disclosure of these vulnerabilities, VIAVI initiated a review across our product portfolio to determine whether any products are affected and to identify any required remediation actions. Product teams are working closely with Engineering, Product Management, and Security teams to complete assessments and deploy mitigations or software updates where necessary.

At this time, we are not aware of any customer-impacting exploitation involving VIAVI products. Assessments remain ongoing, and this advisory will be updated as new information becomes available. Our current product assessment status and recommended customer actions can be found below.

Please do not hesitate to contact us should you require further clarification.

Regards,
Vasanth Madhure
VIAVI CIO

Current Product Assessment Status

Line	Product	Status	Comments
AMS	NITRO GEO	Not Impacted	
	NITRO LI	Not Impacted	
	NITRO CORE	Not Impacted	
	NITRO Mobile	Fix imminent	Fix releases available by Mon 26 Oct 2026: NM 6.0 MR1; NM 6.1 MR2; NM 6.1 MR3
	NITRO AIOPS	Not impacted	
A&D	All Other Products	Not Impacted	
	QG2	Fix under development	Software remediation is under development; Date TBD
FAS	FAS XPT	Not Impacted	
	Fusion	Not Impacted	
	ONMSi	Not Impacted	
	SSPLT	Not Impacted	
	Verity	Not Impacted	
	Fiber Sensing	Not Impacted	
	StrataSync	Fix available	Fix applied on 10/22/2026
	FTH-9000	Fix available	Software update 25.7.60 is available with a fix

	FTH-7000	**Fix available**	Software update 25.7.60 is available with a fix
	FTH-5000	**Fix Available**	Software update 25.7.60 is available with a fix
	OTU-8000 / OTU-8000e	**Fix Imminent**	Customers are advised to disable the web interface when not required. Software remediation is under development.
	METRO (ONA, 5800)	Not Impacted	
L&P	Avalanche	**Not impacted**	
	ONE LabPro	**Fix Imminent**	Fix will be provided in 5.3 planned Oct 30.
	ONT	**Fix Imminent**	Immediate Workaround: Remove Connection from Public Networks. Fix will be provided in ONT Release 50 forecasted for Dec 2026
	FoPLT	Not Impacted	
	Testcenter	Not Impacted	
	AION	Not Impacted	
	CST	Not Impacted	
NPTS	Observer GigaStore	Not Impacted	
	Observer GigaFlow	Not Impacted	
WES	EVOIA	Not Impacted	
	XEdge	Not Impacted	
	QATS	Not Impacted	Customers on older, unsupported systems using Zabbix may be impacted.
WSA	TM500	**Fix available**	RDA Patch will be available on Monday 10/26 and can be applied in the field directly.
	ORU Tester	**Fix under development**	Working with R&S to include the fix (Date TBD). Immediate Workaround: Do not use Web Interface
	TeraVM - RDA / Classic	**Fix available**	RDA 16.11.2 with the fix will be available Monday 10/26
	Xhaul Advisor	Not Impacted	
	VAMOS	Not Impacted	
	TeraVM Oran Security, Knowledge Agent, MCP, AI RSG	Not Impacted	
	Cyberflood	Not Impacted	
	ONA-800 WFI	Not Impacted	
	Ran2Core CU EMU, SIM Test, Core Test	Not Impacted	
	Vertex	Not Impacted	
	Antenna Test	Not Impacted	
OSP	All products	Not impacted	

Recommended Customer Actions

For products identified as impacted, VIAVI recommends that customers:

- Apply software updates when they become available.
- Restrict or disable unnecessary web interface access where operationally feasible.
- Follow any additional product-specific guidance provided by VIAVI Support.
- Contact their VIAVI representative or Technical Support team with any questions regarding their deployment.

Ongoing Monitoring

VIAVI continues to assess all products and associated third-party software components for potential exposure to these vulnerabilities. This advisory will be updated as additional product reviews are completed and remediation activities progress.

For questions regarding a specific VIAVI product, please contact your VIAVI representative or Technical Support.