Vulnerability Disclosure

Table of contents

1. Information 1
2. Product Identification 1
3. Vulnerability Description 2
4. Impact of Vulnerability 2
4.1. Classification and impact 2
4.2. Fix / Mitigation / Remediation 2
5. Contact Information 3
6. Revision History 3

1. Information

Title	Vulnerability Disclosure
Revision	1.0
Issue Date (dd-mmm-yyyy)	23-Oct-2026

The WISI Product Security Incident Response Team (PSIRT) has determined a security vulnerability for the products listed in the Product Identification section of this document.

The information contained within this document describes the identified vulnerability, the classification and impact, the mitigation and remediation.

The information contained within this document has been provided to you, the WISI customer, and you are obliged to provide this information to your customers and inform them that it is their obligation to inform their customers about this Vulnerability Disclosure.

2. Product Identification

Affected Product(s)	GN50W0048, GN50W0110, GN50W0230 GT01W0048, GT01W0110, GT01W0230 ➔ GT11-Module (up to version 3.4.1).

3. Vulnerability Description

CVE-2026-109619	PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE). [https://nvd.nist.gov/vuln/detail/cve-2026-109619]
CVE-2026-109618	PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE). [https://nvd.nist.gov/vuln/detail/cve-2026-109618]

4. Impact of Vulnerability

4.1. Classification and impact

CVE ID	CVSS Vector	CVSS Sore
CVE-2026-109619	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	9.2 Critical
CVE-2026-109618	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	9.2 Critical

Successful exploitation of this vulnerability will compromise to systems' Confidentiality, Integrity, and Availability.

At the time of publication, we are not aware of any active exploitation affecting our products.

4.2. Fix / Mitigation / Remediation

- GT01Wxxxx: Update GT11 to version 3.5 or higher
- GN50Wxxxx: Update to version 3.5 or higher

5. Contact Information

Contact WISI	https://support.wisiconnect.tv
eMail	info@wisigroup.com

6. Revision History

Revision	Date (dd-mmm-yyyy)	Changes
1.0	23-Oct-2026	Initial Release