ASUS Product Security Advisory

We take every care to ensure that ASUS products are secure in order to protect the information security privacy of our valued customers. We constantly strive to improve our safeguards for security and personal information in accordance with all applicable laws and regulations, and we welcome all reports from our customers about product-related security or privacy issues. ASUS strives to adhere to the principles of Coordinated Vulnerability Disclosure (CVD) and actively collaborates with partners to address potential vulnerabilities. Any information you supply to ASUS will only be used to help resolve the security vulnerabilities or issues you have reported. This process may include contacting you for further relevant information. Once the vulnerability report is confirmed, ASUS will notify the submitter as soon as possible and provide timely updates on the handling status.

ASUS PSIRT Participation

ASUS places a high priority on the security of its products and services. We und erstand that security is not a one-time effort, but a continuous commitment. Th

erefore, ASUS continues to work closely with industry partners, academic researchers, and cybersecurity experts, adhering to the best practices outlined in ISO 29147:2018 and ISO 30111:2019 for vulnerability management and handling, while also seeking new ways to enhance the security of our products. As a partner in the CVE Numbering Authority (CNA) program, ASUS follows Coordinated Vulnerability Disclosure (CVD) best practices to ensure timely and responsible resolution of any reported security issues. Additionally, as a member of the Forum of Incident Response and Security Teams (FIRST), ASUS adheres to the PSIRT Framework to systematically address potential security issues reported to ASUS. We encourage customers to take critical security measures, such as following best security practices, keeping products updated, and applying the latest firmware and software patches to ensure that ASUS products always provide a secure and reliable experience.

Latest Security Updates

Title	Type	Affected Products	CVE	Published Date	Last Updated

RSS Subscription

Vulnerability Disclosure Policy

Responsible reporting guidelines:

ASUS appreciates all contributions from customers and the wider ASUS community that help to improve the security of our products and services. However, we kindly request that you act responsibly and bear in mind the following when investigating or reporting any issues:

1. Do not attempt to access or modify any ASUS services, systems, products or software without authorization.
2. Do not disclose, or modify, destroy or misuse any data you may discover.
3. All information given to or received from any party relating to the reported issues must remain completely confidential.
4. Please do not engage in DoS attacks or any destructive testing that may affect the confidentiality, integrity or availability of information and systems.
5. Refrain from participating in social engineering or phishing activities targeting customers or employees.
6. Requests for compensation regarding the time and resources spent verifying vulnerabilities, or for discovered vulnerabilities, will not be considered.

Excluded Submission Types

We always prioritize security and encourage researchers to submit all potential security issues. Each report will be carefully reviewed. However, the following vulnerabilities (including but not limited to) have a very low impact on the system or user security. ASUS will handle and respond to submissions at its discretion based on the circumstances.

- Outdated software versions that contain known vulnerabilities in libraries (e.g., jQuery), leading to low-impact security risks
- Inadequate rate limiting or the absence of CAPTCHA verification mechanisms
- Missing or incomplete SPF, DMARC, or DKIM records

- Cookies not properly configured with HTTPOnly or Secure flags
- Vulnerabilities that only affect outdated or unpatched browsers, extensions, and other non-ASUS software
- Automated tool reports based solely on tool-generated findings, without further analysis of the vulnerabilities
- Exposure of publicly accessible files or directories (e.g., robots.txt)
- Low-risk issues related to clickjacking or UI elements (e.g., problems that are only exploitable through clickjacking)
- Displaying stack traces on error pages instead of generic error messages
- Disclosure of technology or component information (e.g., PHP,ASP.NET usage)
- Account or email enumeration with no significant impact on the security of ASUS services or products
- Absence of non-mandatory security headers, where the lack does not lead to an exploitable vulnerability
- Insufficient HTTP security settings, where the specific impact (such as data leakage or functionality abuse) cannot be demonstrated
- Low-risk CSRF issues (e.g., login, logout, or minor unauthenticated cross-site request forgery vulnerabilities)

How to report a security vulnerability or issue to ASUS

We welcome all reports related to security incidents concerning ASUS. We invite you to contact us about such matters through our dedicated web form: **https://www.asus.com/securityadvisory**. By submitting a vulnerability report, you acknowledge and accept ASUS's vulnerability submission policy.

To help us address your concerns quickly, please ensure you provide the following information on the website.

1. Your full name and a means of contacting you. This can be an email address or any other preferred method we can use to get in touch with you.
2. Full and detailed information about the issue you wish to report. This should include the following information, as applicable:
    - The name of the ASUS service(s) or system(s) that your concern relates to.

- The name, description and version number of any affected ASUS software products.
- A full and detailed description of the problem or issue, along with any background information that you believe is relevant, and any other pertinent information that may help us reproduce and/or resolve the issue. Finding Vulnerabilities (Problems) Step-by-Step Instructions for Reproducing the Vulnerability Technical Description of the Vulnerability (Including Proof of Concept, if possible) Potential Impact of the Vulnerability Any Other Information That Can Help Us Reproduce and Resolve the Issue
- Methods for discovering vulnerabilities or issues
- Detailed steps for reproducing the vulnerability
- Technical description of the vulnerability (if possible, including proof of concept)
- Potential impact of the vulnerability
- Any additional information that could help us reproduce and resolve the issue

We encourage you to use encrypted communication to protect the confidentiality of your information. You can encrypt your report using the PGP public key provided below:

PGP Public Key

Expand Click to copy 🔗

What happens next?

Once we have resolved the reported issue(s), we will provide a suitable solution to all affected customers. We will treat this with the utmost priority and make the solution available as soon as it practical to do so.

ASUS will also maintain a list of the latest software updates, along with descriptions of the issues that have been fixed. Although we will notify customers wherever possible, we also recommend that customers visit this page regularly to make sure they are aware of the latest updates.

Hall of Fame

2026 2025 2024 2023 2022 2021 2020 2(

March

- Gu YongZeng (@0x0dee) working with TrendAI Zero Day Initiative
- Zhihong Liu (@vincebye)

January

- Yohan Seok (@seokjohn) with JENBlack Soft

Disclaimer

All aspects of the ASUS PSIRT (Product Security Incident Response Team) processes and policies may be adjusted based on specific circumstances and are subject to change without prior notice. We do not guarantee a response to any particular issue or category of issues. The use of the information in this document or any related links is at your own risk.

Contact Us

If you have any questions, concerns, feedback, or complaints regarding our Privacy Policy, or if you believe that ASUS has not complied with it, please do not hesitate contact us through 📧 **privacy@asus.com**.