Vulnerability Research & Advisor

The Coordinated Vulnerability Disclosure (CVD) process has been in place in the TIM Cyber Security department since 2019 and has been integrated into ethical hacking and bug hunting activities.
The Coordinated Vulnerability Disclosure represents an ethical approach to disclosing zero-day vulnerabilities, i.e., security bugs that are still unknown to developers and potentially exploitable before dedicated patches are released.
Through this process, the bug hunter discloses the identified vulnerabilities to vendors confidentially, granting them time to implement a security patch before the public disclosure.
This method strengthens the collective response to cyber threats, reducing the risk of malicious actors exploiting these critical vulnerabilities.
At TIM, we continuously work to promote the responsible disclosure of vulnerabilities, supporting vendors in identifying and resolving emerging threats and offering numerous benefits, such as:

- System administrators are incentivized to promptly install security patches once bugs are made public;
- Perimeter protection vendors can update their policies to intercept and block new malicious payloads;
- Vulnerability Assessment tool vendors can update their products to detect new vulnerabilities;
- Other vendors have the opportunity to verify whether the same criticality affects their own products, such as in open-source libraries.

This page compiles and updates the bug hunting work done by TIM: vulnerabilities are disclosed to public only after the vendor has released the security patch and agreed to share the details.
This approach helps build a more secure and collaborative ecosystem, both nationally and internationally, where responsible vulnerability sharing becomes a fundamental pillar in the fight against cyber threats.

2025

CVE-2025-5459 – Puppet Enterprise

CVE-2025-23366 – WildFly

CVE-2025-23367 – WildFly

CVE-2025-23368 – WildFly

CVE-2025-24948– JotUrl

CVE-2025-24949– JotUrl

CVE-2025-30694 – Oracle XML DB 9i

CVE-2025-1534 – Payara Server Community

CVE-2025-27258 - Ericsson Network Manager

CVE-2025-27259 - Ericsson Network Manager

CVE-2025-47904 - Microchip TP4100

CVE-2025-47902 - Microchip TP4100

CVE-2025-47901 - Microchip TP4100

CVE-2025-47900 - Microchip TP4100

CVE-2025-12453 - OpenText Vertica

CVE-2025-12454 - OpenText Vertica

CVE-2025-12455 - OpenText Vertica

CVE-2025-9497 - Microchip TP4100

CVE-2025-24817 - Nokia MantaRay NM

CVE-2025-24818 - Nokia MantaRay NM

CVE-2025-24819 - Nokia MantaRay NM