




CENTRE FOR
CYBERSECURITY
BELGIUM

FLASH REPORT



WARNING: ACTIVE EXPLOITATION OF IVANTI CONNECT SECURE EOL DEVICES!

CYBER THREAT INTELLIGENCE REPORT

Date: 15 April 2025
Version: 1.0 EN
Author: The CCB (CyTRIS, intelligence (CTI) department)

Target audience:
Organisations using Ivanti devices

Permitted distribution of TLP:CLEAR:
Recipients can spread this to the world, there is no limit on disclosure.
More information: <https://www.first.org/tlp/>

Table of Contents

Executive summary 4

Recommendations 4

- Check vulnerable versions 4
- Ivanti external Integrity Checker **Error! Bookmark not defined.**
- Check your environment for traces of compromise 4
- Report incidents and threat information 4

References 5

About the CCB 5

EXECUTIVE SUMMARY

The Centre of Cybersecurity Belgium (CCB) was informed about multiple compromises of Ivanti End-Of-Life devices. These End-Of-Life devices were used as initial access point for threat actors to further compromise the internal network. It is not possible to patch these End-of-Life devices.

With this alert, the CCB wants to engage security teams to thoroughly check these devices and the entire network, start incident response if necessary and inform the CCB on <https://ccb.belgium.be/cert/report-incident>.

RECOMMENDATIONS

The CCB recommends to perform the following actions as soon as possible:

Patch your Ivanti devices, replace them when End-of-Life

Please check the current running version of your Connect Secure devices, affected software:

- Pulse Connect Secure 9.1R18.9 and prior (END OF LIFE)
- Ivanti Connect Secure 22.7R2.5 and prior
- Ivanti Policy Secure 22.7R1.3 and prior
- ZTA Gateways 22.8R2 and prior

The CCB strongly advises owners of End-of-Support devices to contact Ivanti to migrate to a secure platform. If a patch is available for your device, please patch with the highest priority.

Check for compromises with the Ivanti external Integrity Checker

Run the Ivanti external Integrity Checker Tool (ICT) to detect signs of compromise. Take into account following limitations: the ICT offers a snapshot of the current state of the appliance and cannot necessarily detect threat actor activity if the appliance has been returned to a clean state. The ICT does not scan for malware or IoCs.

Check your environment for traces of compromise

Thoroughly scan your environment for any suspicious behaviour. If your organization is connected to our MISP community or another connected community, the information is available with UUID db5f885b-7a82-4952-b138-956e39033df0. You can also [download indicators here](#). This is based on the public references below.

Report incidents and threat information

If you encounter a similar incident (or encountered such incident in the past), please notify us by using our reporting form (<https://ccb.belgium.be/cert/report-incident>). For urgent cases, you can also reach us by phone on +32 (0)2 501 05 60.

REFERENCES

CCB advisory CVE-2025-22457: <https://ccb.belgium.be/advisories/warning-actively-exploited-critical-remote-code-execution-vulnerability-ivanti-products>

<https://www.cisa.gov/news-events/alerts/2025/03/28/cisa-releases-malware-analysis-report-resurge-malware-associated-ivanti-connect-secure>

<https://www.cisa.gov/news-events/analysis-reports/ar25-087a>

<https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day>

ABOUT THE CCB

The **Centre for Cybersecurity Belgium (CCB)** is the national authority for cybersecurity in Belgium. The CCB supervises, coordinates and monitors the application of the Belgian cyber security strategy. Through optimal information exchange, companies, the government, providers of essential services and the population can protect themselves appropriately.

The Centre for Cybersecurity Belgium (CCB) was established by Royal Decree of 10 October 2014 and operates under the authority of the Prime Minister.

The **CyTRIS (Cyber Threat Research and Intelligence Sharing)** Department of the Centre for Cybersecurity Belgium monitors cyber threats and publishes regular reports. The Team collects, analyses and distributes information on threats, vulnerabilities and attacks on the information and communication systems of Belgium's vital sectors (critical infrastructure, government systems, critical data).

CyTRIS is also responsible for the Early Warning System (EWS). The EWS includes the information exchange platforms of the Belgian CSIRT. CyTRIS is responsible for the operational communication and information exchange with other national CSIRT. CyTRIS also provides the "Spear Warning" procedure. A "Spear Warning" is an individual warning about an infection or vulnerability sent to organisations.

The CCB Connect & Share events, such as the Quarterly Cyber Threat Report (QCTR) events organised by CyTRIS, bring together different stakeholders and consultation platforms at least once a quarter and inform all participants as well as the Organisations of Vital Interest about the active cyber threats. At the QCTR event, the operation of the Early Warning System (EWS) is also discussed. Through this platform, the CyTRIS Team sends pertinent and analysed threat information to national security agencies, Vital Interest Organisations, their sectoral authorities and other partners.

Our events are also offered as a webinar and are open to anyone, for prior editions check out our YouTube channel: <https://www.youtube.com/@cybersecuritybelgium>.