NTS SUPER SERVICES

NTS VULNERABILITY MODUL

NTS RELAX, WE CARE

NTS VULNERABILITY MODUL

Many networks will most probably have a security vulnerability that can be exploited. To prevent security problems and vulnerabilities, it is a crucial and constant task for businesses to identify vulnerabilities, to track them and to counter them.

Manual controlling and checking are very often difficult to implement under real conditions and it is required to find means for an efficient, simple and fast identification of possible gaps in the infrastructure of the network.

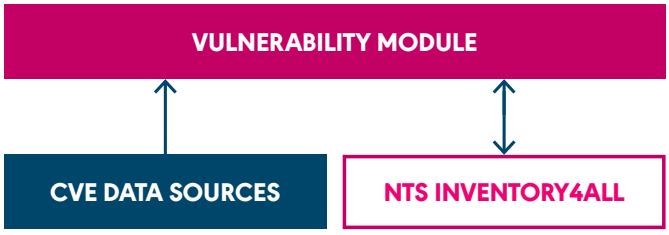
With its Cisco Product Security Incident Response Team (PSIRT), Cisco provides a dedicated team that receives, investigates and publicly discloses information about security vulnerabilities in connection with Cisco products and networks. The PSIRT assigns CVE (Common Vulnerabilities and Exposure) labels to vulnerabilities that have been found internally and externally in hundreds of products. In addition, other manufacturers also provide CVEs. The challenge lies in the task to identify and to administer relevant CVEs for the network inventory. With the Vulnerability Module as an add-on for NTS INVENTORY4ALL (I4ALL), NTS offers its customers a suitable solution for the reduction of risks for open vulnerabilities in their own network inventory.

With the Vulnerability Module, the customers receive a quick overview of open CVEs on their devices. The disclosed CVEs with information about severity, CVSS Score[1] and date of disclosure will be displayed in the CVE list. Amongst others, a description of the CVE itself can be found in the CVE details.

YOUR ADVANTAGES AT A GLANCE

- Quick overview of all devices that are affected by CVEs
- Increase of the network security and conformity
- Risk reduction through CVEs for their own network inventory
- Customer-specific matching of vulnerabilities and devices
- Efficiency increases during operation due to clear displays
- Proof available to third parties (e.g., auditor, authorities) about the risk development
- Proactive notification for CVEs according to the set rules
- Vulnerability Module as a building block for the NIS set of measures

The devices in the network that are affected by CVE[2] are also shown. Moreover, this allows to navigate it to the respective device in I4ALL in order to check if the CVE is relevant and to derive necessary measures if necessary. Thus, the Vulnerability Module is the suitable tool for vulnerability and risk management that is built on it.



Interaction with I4ALL and CVE data sources

[1] The Common Vulnerability Scoring System (CVSS) is a standard for the assessment of IT security vulnerabilities.
[2] The matching is made on the basis of a model and software version of the hosts that are attended to in NTS INVENTORY4ALL

RELAX, WE CARE

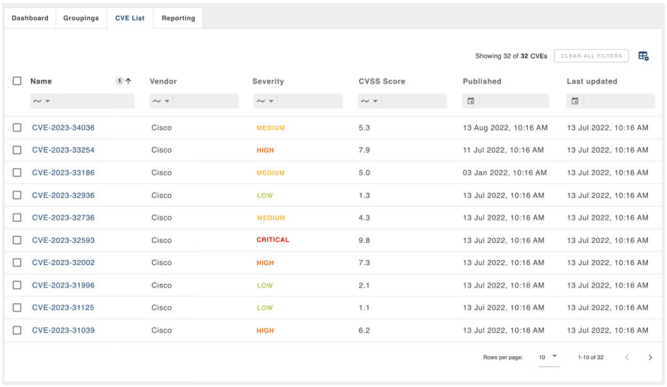
You're never left alone as we assume the responsibility for monitoring your systems, processes, and their analysis. Precisely to the extent that you require, just in that style that you desire.

→ **www.nts.eu**

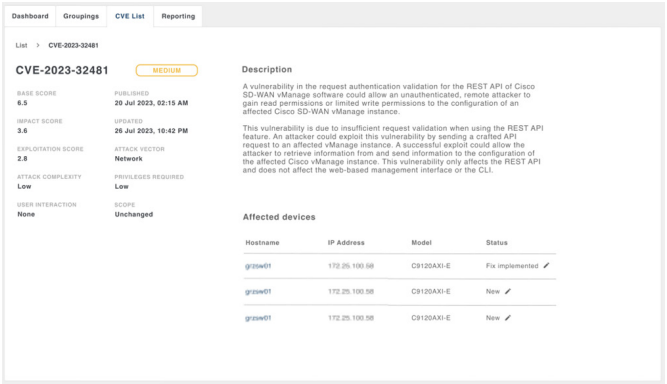
NTS VULNERABILITY MODUL

REPORTING AND ALERTING

Don't want to miss any new CVEs and you want to keep an eye on everything? NTS has the answer in the form of the integrated reporting and alerting functionality. Status reports can be compiled in an automated manner at defined intervals, and they can be provided as a PDF file. Automated email notifications based on preset rules (e.g., CVSS score >7 for switches) support the customer-specific alert system.



CVE list



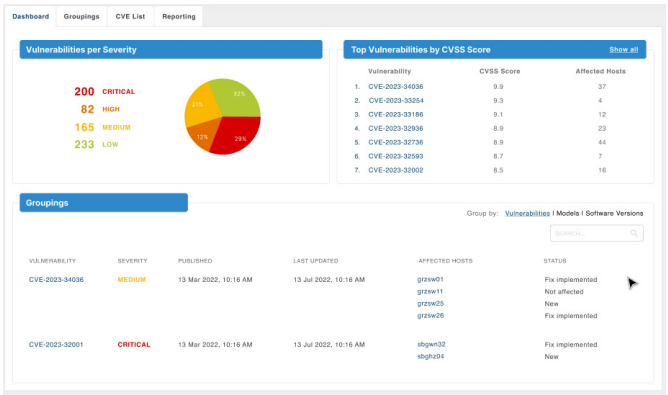
CVE details

For the efficient processing as well as for the risk management, the Vulnerability Module provides, along with the CVE list and dashboard, a clear display that is grouped by vulnerabilities or by module/software version supplemented by possibilities to sort and to filter. It indicates, for example, a particular CVE for the affected hosts. This allows critical CVEs and affected devices to be quickly identified, analyzed and measures derived.

In addition to the displays in the Vulnerability Module, the host details in I4ALL also provide vulnerability information. The CVEs found are displayed here and the user can maintain the status for each CVE on the host (e.g.: Workaround implemented, not affected). Thus, implemented measures and status changes are documented.

DASHBOARD AND KPIS

A dashboard with KPIs completes the scope of services. It provides the user with clear displays, for instance, for vulnerabilities per severity or top vulnerabilities by CVSS score. A trend chart shows the time sequence of all devices that are affected by vulnerabilities. This can serve as proof to external parties of the risk management in your own network.

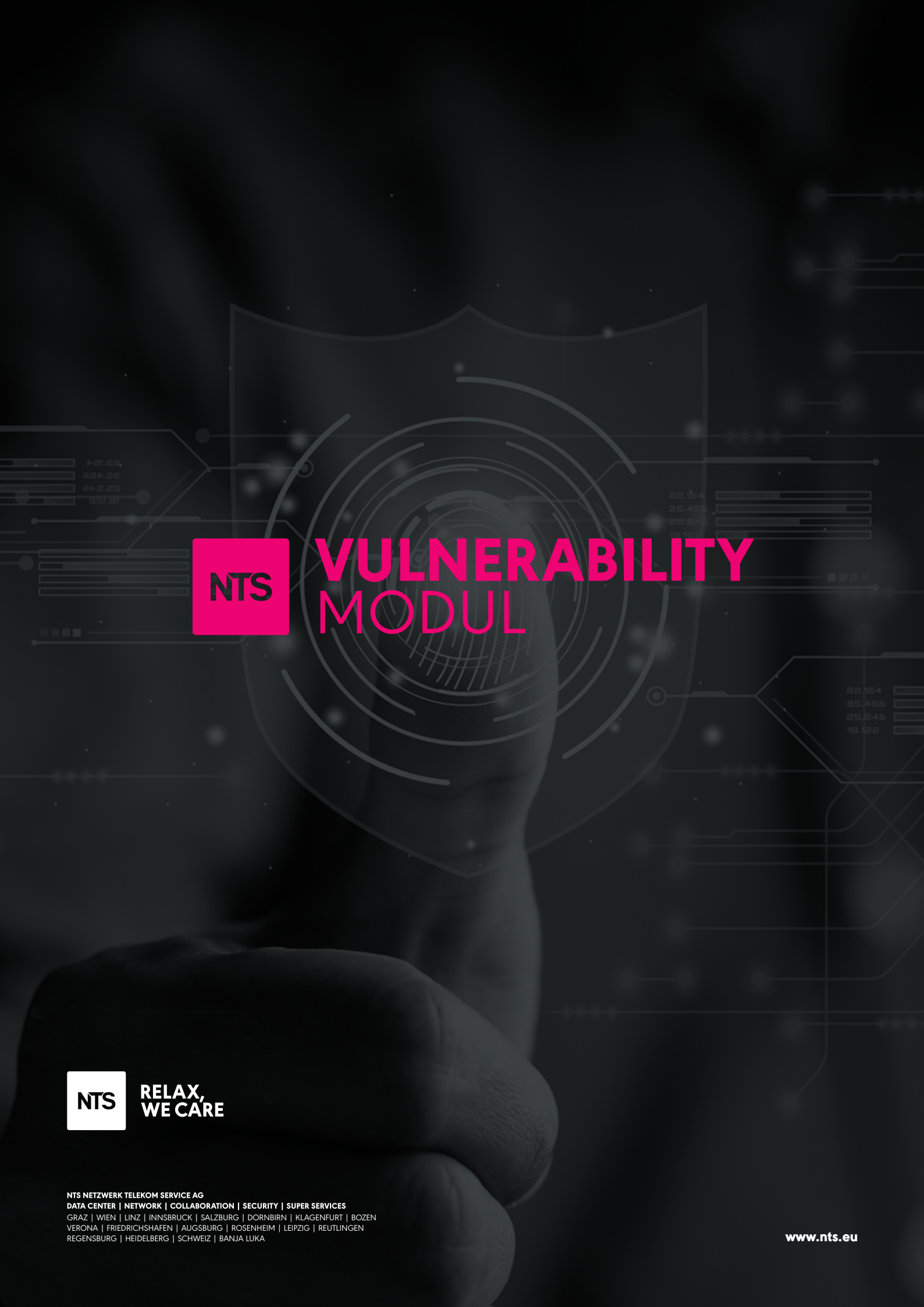


Dashboard

RELAX, WE CARE

You're never left alone as we assume the responsibility for monitoring your systems, processes, and their analysis. Precisely to the extent that you require, just in that style that you desire.

→ **www.nts.eu**



VULNERABILITY MODUL

RELAX, WE CARE

NTS NETZWERK TELEKOM SERVICE AG
DATA CENTER | NETWORK | COLLABORATION | SECURITY | SUPER SERVICES
GRAZ | WIEN | LINZ | INNSBRUCK | SALZBURG | DORNBIRN | KLAGENFURT | BOZEN
VERONA | FRIEDRICHSHAFEN | AUGSBURG | ROSENHEIM | LEIPZIG | REUTLINGEN
REGENSBURG | HEIDELBERG | SCHWEIZ | BANJA LUKA

www.nts.eu