DAIMLER TRUCK

Daimler Truck CSOC RFC 2350

1. Document information

This document presents a public overview of the Daimler Truck Cyber Security Operation Center (CSOC) in accordance with RFC 2350 guidelines. It furnishes fundamental details regarding the CSOC outlines methods for contacting the center, and delineates its core responsibilities.

1.1 Date of last update

2024-10-01, 16:17 (CET)

1.2 Distribution list for notifications

There is no public distribution list for notifications.

1.3 Locations where this document may be found

The current version of this document can always be found at:
https://www.daimlertruck.com/en/vulnerability-reporting-policy

1.4 Document authenticity

This document can be retrieved from our webserver using TLS/SSL.

2. Contact information

2.1 Name of the team

Daimler Truck CSOC

2.2 Address

Daimler Truck AG
Fasanenweg 10
70771 Leinfelden-Echterdingen
Germany

2.3 Time zone

We operate within the Central European Time Zone (CET), equivalent to GMT+0100 (or GMT+0200/CEST during European summertime, typically observed from the end of March until the end of October).

2.4 Telephone numbers

International: +800-8485-7777

2.5 Facsimile number

None.

2.6 Other telecommunication

None.

2.7 Electronic mail address
None

2.8 Public keys and encryption information
Not Required for Incident Reporting since Daimler Truck is having specified Report Submission Form available : Daimler Truck Report Submission Form

3. Charter

3.1 Mission statement
Establish and maintain a robust Cyber Security Operation Center (CSOC), swiftly identifying, analyzing, and addressing cybersecurity incidents to protect our assets, data, and operations, thus safeguarding the security and integrity of our digital infrastructure.

3.2 Constituency
Daimler Truck CSOC constituency are all entities of Daimler TruckGroup.

3.3 Sponsorship and/or affiliation
Daimler Truck CSOC operates as an internal unit within the Daimler Truck Group, solely financed and empowered from the organization's group Chief Information Security Officer (CISO).

3.4 authority
The primary objective of Daimler Truck CSOC is to centrally coordinate incident response and operational incident handling across Daimler Truck subsidiaries and affiliated companies on a multinational scale. Consequently, our role is advisory, and we do not possess the authority to mandate specific actions.

4. Policies

4.1 Types of incidents and level of support
Daimler Truck CSOC deals with various security incidents that arise or pose a threat within its constituency. The extent of assistance provided depends on the nature of the security incident, its impact on affected entities within our constituency, and our available resources. Typically, our initial response occurs promptly within two working days.

4.2 Co-operation, interaction, and disclosure of information
Daimler Truck CSOC places significant importance on fostering operational collaboration and sharing information with other Security Teams and relevant organizations that may benefit from or contribute to our services.

The Daimler Truck CSOC operates in strict compliance with local and international laws and regulations, collaborating closely with corporate security to uphold data protection standards.

4.3 Communication and authentication
Daimler Truck CSOC makes use common cryptographic methods to ensure the confidentiality and integrity of the communications.

5. Services

5.1 Incident response

The Daimler Truck CSOC can handle operational incidents across various environments 24/7. This involves various tasks such as conducting large-scale threat hunting and security incident detection, gathering artifacts, analyzing artifacts, assessing threat intelligence, and analyzing malware.

5.2 Incident coordination

Daimler Truck CSOC maintains operational capabilities to effectively coordinate high-severity cybersecurity incidents and emergencies. Additionally, Daimler Truck CSOC will compile incident statistics within its jurisdiction to facilitate reporting.

5.3 Proactive activities

Daimler Truck CSOC provides current information on security vulnerabilities and potential threats to its internal stakeholders. Furthermore, the team consistently innovates by developing novel techniques for detecting and investigating incidents.

6. Incident reporting forms

We request you to submit your Vulnerability report at Daimler Truck Incident Report Submission Form and also have a look at our Vulnerability Disclosure Program (VDP) which a structured process that enables security researchers and the public to report security vulnerabilities in an organization's systems. It aims to improve security by facilitating the identification and remediation of vulnerabilities in a legal and efficient manner. Vulnerability Reporting Policy | Daimler Truck

7. Disclaimers

Although every effort will be made to ensure accuracy in the preparation of information, notifications, and alerts, Daimler Truck CSOC disclaims any responsibility for errors or omissions, or for damages arising from the use of the information provided.