Mercedes-Benz CIRC RFC2350

1. Document information

This document contains a public description of Mercedes-Benz Cyber Intelligence and Response Center (CIRC) according to RFC 2350. It provides basic information about the CIRC, the ways it can be contacted and describes its responsibilities.

1.1 **Date of last update**

09 Feb 2023, 12:00:00 (UTC+1)

1.2 **Distribution list for notifications**

There are no public distribution list for notifications as of 2023/02.

1.3 **Locations where this document may be found**

The current version of this document can always be found at:
https://www.mercedes-benz.com/en/whitehat

1.4 **Document Authenticity**

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

2. Contact information

2.1 **Name of the team**

Mercedes-Benz CIRC

2.2 **Address**

Mercedes-Benz AG
Mercedesstraße 120
70372 Stuttgart
Germany

2.3 **Time zone**

Mercedes-Benz CIRC is located in multiple time zones due to our follow-the-sun approach:
Germany: UTC +1
Singapore: UTC +8
Canada: UTC -5

2.4 **Telephone numbers**

None.

2.5 **Facsimile number**

None.

2.6 **Other telecommunication**
None.

2.7 **Electronic mail address**
Please send incident reports to **security@mercedes-benz.com**.

2.8 **Public keys and encryption information**
Please request our public PGP or S/MIME keys here:
https://webmail.daimler.com/responsiveUI/requestPublicKey/requestPublicKey.xhtml

3. Charter

3.1 Mission statement

Protect Mercedes-Benz and its constituents from attacks, using state-of-the-art detection and prevention methods. Effectively manage cyber incidents and ensure the timely and sustainable resolution and recovery.

3.2 Constituency

Mercedes-Benz CIRC constituency are all entities of Mercedes Benz Group.

3.3 Sponsorship and/or affiliation

Mercedes-Benz CIRC is an internal unit of Mercedes Benz Group and is solely financed and supported by the latter.

3.4 Authority

The main purpose of Mercedes-Benz CIRC is the group-wide and multinational coordination of incident response and operative incident handling, throughout Mercedes-Benz subsidiaries and member companies. As such, we can only advise our constituency and have no authority to demand certain actions.

4. Policies

4.1 Types of incidents and level of support

Mercedes-Benz CIRC addresses all kinds of security incidents which occur, or threaten to occur, within its constituency.
The level of support depends on the type and severity of the given security incident, the impact for affected companies and persons within our constituency, and our resources at the time. Usually, our first response is timely at the same working day.

We expect end users to contact their local information security contacts (ISO).

4.2 Co-operation, interaction and disclosure of information

Mercedes-Benz CIRC highly regards the importance of operational cooperation and information-sharing between other Security Teams, and also with other organizations which may contribute towards or make use of their services.
Mercedes-Benz CIRC operates in strict compliance with German and/or international legislation.

4.3 Communication and authentication

Mercedes-Benz CIRC makes use common cryptographic methods to ensure the confidentiality and integrity of the communications. PGP and S/MIME are available for general communication via email.

5. Services

5.1 Incident response

Mercedes-Benz CIRC is able to perform operative incident handling in several different environments. The tasks include large-scale threat hunting and detection of security incidents, artifact collection, artifact analysis, threat intelligence and malware analysis.

5.2 Incident coordination

Mercedes-Benz CIRC ensures it has operational capabilities to coordinate high-severity cyber security incidents and emergencies. Mercedes-Benz CIRC will also collect statistics about incidents within its constituency to enable reporting.

5.3 Proactive activities

Mercedes-Benz CIRC offers up-to-date information about security vulnerabilities and possible threats to its internal constituents. Besides, the team continuously develops new methods for incident detection and investigation.

6. Incident reporting forms

There are no public forms available. All communication should be directed to **security@mercedes-benz.com**. We recommend any communication related to security incidents or vulnerabilities to be encrypted by PGP or S/MIME. Please request our public key here:
https://webmail.daimler.com/responsiveUI/requestPublicKey/requestPublicKey.xhtml

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, Mercedes-Benz CIRC assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.