

报告 DRÄXLMAIER 产品或 IT 系统中的漏洞



报告 DRÄXLMAIER 产品或 IT 系统中的漏洞

如果您发现了我们产品或IT系统中的潜在安全漏洞，请通过发送电子邮件至我们的邮箱 cert@draexlmaier.com 报告给我们。

电子邮件中需要包含以下信息，以便我们以最佳方式跟进您的消息：

1. 消息主题

如果这是我们产品中存在的潜在安全漏洞，请在主题行中写上“报告可能存在的汽车网络安全/产品安全漏洞”。另一方面，如果这是我们IT系统中的漏洞，请在主题行中写上“报告可能存在的信息安全漏洞”。

2. 语言

请用英语或德语发送信息给我们。

3. 联系

为了处理您的消息，我们需要您的联系方式。请注意有关数据保护的信息。

4. 关于重现漏洞的信息

为了能够重现潜在的安全漏洞，我们需要您提供足够的信息：

- 潜在安全漏洞的详细描述以及如何发现它。
- 受潜在安全漏洞影响的产品（例如组件名称、部件编号、软件版本）或IT系统（例如名称、IP地址、软件）。
- 您首次发现潜在安全漏洞的时间。
- 发现潜在安全漏洞所需满足的条件。

所有提供的信息当然会被保密处理。

如果与汽车网络安全/产品安全领域或信息安全中的安全漏洞有任何关联，我们将在收到您的消息后72小时内与您联系。

感谢您的合作。

数据保护信息

根据 GDPR 第 4 条第 7 款，数据的所有者是 Lisa Dräxлмаier GmbH，位于德国84137Vilsbiburg Landshuter Straße 100。公司的数据保护官可以通过以下地址联系：

数据保护官，地址是 Lisa Dräxлмаier GmbH，位于德国84137Vilsbiburg Landshuter Straße 100，或通过电子邮件 privacy@draexlmaier.com 联系。

当您通过电子邮件与我们联系时，我们处理您提供的联系信息以解决报告的问题，并在必要时进一步联系您。

为此需要一个有效的电子邮件地址，以便我们能够回应您的请求。您也可以自愿提供更多信息。根据 GDPR 第 6 条第 1 款第 1 句 a) 项，数据处理是基于您通过发送数据自愿同意的基础进行的。其目的是处理您提交的关于汽车网络安全/产品安全或信息安全的漏洞报告。我们收集的个人信息将在处理完成后删除，除非法律或其相关原因使我们有权保留更长时间。

我们无意将从您那里收集的个人信息用于自动决策（包括分析）。

您没有义务向我们提供您的数据，但如果没有联系方式，我们无法处理您的电子邮件。

有关您作为数据主体的权利、投诉权、撤回同意权以及数据处理的进一步信息，请参阅数据保护通知 [Data protection \(draexlmaier.com\)](https://www.draexlmaier.com/data-protection)。