奇安信
新一代网络安全领军者

https://www.qianxin.com

智能网联汽车云平台漏洞分析报告

THE REPORT

发布机构：
奇安信代码安全实验室 奇车安全团队

摘　要

- **漏洞问题普遍且严重：**2025 年，奇安信代码安全实验室奇车安全团队对 30 家汽车厂商的云平台进行了漏洞分析，其中 28 家云平台发现了漏洞，漏洞检出率 93.3%，所有云平台总共发现 207 个漏洞，其中超危和高危漏洞共计 66 个，占比 31.9%。
- **高危漏洞存在极高风险：**在分析的 30 家汽车厂商云平台中，有 23 家云平台发现了超危或高危漏洞，占比高达 76.7%。通过验证发现，这些超危和高危漏洞可造成远程解锁车辆、近场解锁车辆、未授权驾驶车辆、敏感信息泄露等严重危害，整体风险极高。
- **低级错误反映出整体安全水平极低：**在总共发现的 207 个漏洞中，有 135 个是因身份未检验、接口未鉴权等低级错误而导致，占比高达 65.2%。反映出行业整体软件安全水平极低，亟须夯实基础。
- **漏洞风险复杂严峻，危害覆盖多个层面：**超七成汽车厂商云平台存在身份认证和访问控制类漏洞，半数汽车厂商云平台存在过度数据暴露漏洞，三成汽车厂商云平台存在数字钥匙管理失效漏洞；超七成汽车厂商云平台存在敏感信息泄露，数据安全风险突出；2/3 厂商的汽车可利用漏洞在未授权情况下解锁，直接危害车辆财产安全；四成汽车厂商云平台存在用户账户被冒用进行未授权操作的安全风险。

目　录

一、概述 1

二、漏洞总体状况分析 1

1、超七成汽车厂商云平台存在超危/高危漏洞，直接危害汽车安全，风险极高 1

2、超六成漏洞因低级错误导致，整体安全水平极低，亟须夯实基础 2

三、主要漏洞类型分析 3

1、超七成汽车厂商云平台存在身份认证和访问控制类漏洞 3

2、半数汽车厂商云平台存在过度数据暴露漏洞 7

3、三成汽车厂商云平台存在数字钥匙管理失效漏洞 9

四、主要漏洞危害分析 10

1、 超七成汽车厂商云平台存在敏感信息泄露，数据安全风险突出 11

2、2/3 厂商的汽车可利用漏洞在未授权情况下解锁，直接危害车辆财产安全 12

3、四成汽车厂商云平台存在用户账户被冒用进行未授权操作的安全风险 13

五、总结及建议 14

附录：奇安信代码安全实验室简介 17

一、概述

随着汽车智能化、网联化的快速发展，智能网联汽车云平台已成为智能网联汽车生态的核心数字基础设施。智能网联汽车云平台的主要功能涵盖数据采集治理、车辆全周期集中管理、实时状态监控、AI 算法迭代训练、车路云协同决策等，是连接车端、路端、用户与外部生态的数字化枢纽，其安全性是智能网联汽车安全的重中之重。

2025 年，奇安信代码安全实验室奇车安全团队对 30 家主流汽车厂商的云平台进行了漏洞分析，并在真实车辆上进行了验证，基于对漏洞分析和验证数据的统计分析，最终形成本报告。报告主要包括智能网联汽车云平台漏洞总体状况分析、主要漏洞类型分析、主要漏洞危害分析、总结及建议等内容，希望可以为相关机构和厂商开展相关研究和实践工作提供有益的参考。

二、漏洞总体状况分析

在分析的 30 家汽车厂商云平台中，有 28 家云平台发现了漏洞，漏洞检出率 93.3%，所有云平台总共发现 207 个漏洞，其中超危和高危漏洞共计 66 个，占比 31.9%。

1、超七成汽车厂商云平台存在超危/高危漏洞，直接危害汽车安全，风险极高

在分析的 30 家汽车厂商云平台中，有 23 家云平台发现了超危或

高危漏洞，占比高达 76.7%。通过验证发现，这些超危和高危漏洞可造成远程解锁车辆、近场解锁车辆、未授权驾驶车辆、敏感信息泄露等严重危害，整体风险极高。

发现超危/高危漏洞最多的云平台发现了 9 个超危/高危漏洞，超危/高危漏洞数量排名前 5 位的云平台如下表所示。

汽车厂商云平台	超危/高危漏洞数量
云平台 1	9
云平台 2	7
云平台 3	7
云平台 4	6
云平台 5	5

2、超六成漏洞因低级错误导致，整体安全水平极低，亟须夯实基础

在总共发现的 207 个漏洞中，有 135 个是因身份未检验、接口未鉴权等低级错误而导致，占比高达 65.2%。在分析的 30 家汽车厂商云平台中，有 19 家存在因此类低级错误而导致的漏洞，占比高达 63.3%，其中 12 家存在因此类低级错误而导致的超危或高危级别漏洞，占比高达 40.0%。

从分析结果来看，因此类低级错误导致的漏洞占比很高，并且是大多数汽车厂商云平台都普遍存在的问题，反映出当前汽车厂商云平台的整体软件安全水平极低，亟须夯实安全基础。

三、主要漏洞类型分析

在总共发现的 207 个漏洞中，主要包括失效的访问控制、过度数据暴露、身份认证失效、会话管理失效、数字钥匙管理失效、命令注入、跨站脚本、业务逻辑漏洞等 8 种类型，其中数量较多的漏洞类型包括失效的访问控制、过度数据暴露、身份认证失效、会话管理失效、数字钥匙管理失效等 5 类。5 类数量较多的漏洞所影响的智能网联汽车云平台的数量及占比情况如下表所示。

漏洞类型	影响云平台数量	影响云平台占比
失效的访问控制	18	60.0%
过度数据暴露	15	50.0%
身份认证失效	13	43.3%
会话管理失效	9	30.0%
数字钥匙管理失效	9	30.0%

1、超七成汽车厂商云平台存在身份认证和访问控制类漏洞

在分析的 30 家汽车厂商云平台中，有 18 家存在“失效的访问控制”漏洞，占比 60.0%，有 13 家存在“身份认证失效”漏洞，占比 43.3%。身份认证和访问控制作为网络信息安全的两大基石，二者紧密关联，共同构筑了系统的安全底座。考虑其内在的强关联性，我们将“失效的访问控制”和“身份认证失效”两类漏洞进行了合并统计，发现两类漏洞共计影响了 22 家汽车厂商云平台，占比高达 73.3%。

身份认证和访问控制类漏洞属于基础性漏洞，是软件安全开发管理流程中的核心必查项，此两类漏洞的大面积存在，绝不仅仅是个别开发人员的疏忽导致，而是源自系统性的流程和管理缺陷。这表明当前大多数汽车厂商在其云平台的开发中，没有建立基本的软件安全开发管理流程，安全架构设计缺位，安全编码规范缺失，代码审计和渗透测试严重不足。

失效的访问控制（Broken Access Control）

失效的访问控制是指应用程序未能实现预期的用户权限控制，即未能对用户的功能权限、数据权限或操作权限进行严格的校验。这使得攻击者能够通过修改请求参数、遍历 URL 或重放数据包等方式，绕过访问限制，访问未授权的资源或执行未授权的操作。

本报告中发现的失效的访问控制类漏洞主要包括：未授权访问、越权访问。

① 未授权访问

定义：绕过登录或权限检查，直接访问敏感资源。

场景示例：攻击者在未登录状态下，直接访问 API 接口或后台管理页面，系统未进行拦截，导致敏感数据泄露、系统控制权丢失和业务功能滥用等危害（如 API 接口未鉴权）。

② 越权访问

定义：系统未能正确校验用户是否具备执行某项操作或访问某个资源的权限，导致用户可以操作或访问超出其权限范围的功能或

数据。

场景示例：

- 水平越权：相同权限级别的用户之间互相越权。例如，普通用户 A 通过修改请求中的 ID 参数（如将 user_id=1001 改为 user_id=1002），查看或修改普通用户 B 的私有数据（如查看其姓名、手机号、地址）。
- 垂直越权：低权限用户向高权限用户越权。例如，普通用户通过直接访问管理员接口（如/admin/deleteUser）或修改角色参数（如 role=user 改为 role=admin），执行管理员才能执行的操作（如删除数据、修改配置）。

身份认证失效（Authentication Failures）

身份认证失效是指系统在验证用户身份的核心环节存在逻辑或技术缺陷，导致攻击者能够伪造凭证、绕过校验或暴力破解，从而非法获取系统访问权限。

本报告中发现的身份认证失效类漏洞主要包括：身份认证绕过、验证码机制失效、账号枚举、弱口令与默认凭证。

① 身份认证绕过

定义：攻击者利用系统逻辑缺陷，无需提供有效凭证即可直接访问受保护资源。

场景示例：通过修改数据包参数（如将 is_verified=0 改为 1）、删除关键校验字段，或利用前端 JavaScript 校验的漏洞，直接跳

过登录/验证步骤进入系统后台。

② 验证码机制失效

定义：用于区分人机的验证码防线被突破，例如验证码校验接口缺少安全控制（如访问间隔、访问次数限制），或合法验证码使用后未能及时进行失效化处理等，导致自动化脚本可以无限次尝试。

场景示例：

- 验证码爆破：验证码位数过短（如 4 位纯数字）或复杂度不足，攻击者通过自动化脚本穷举遍历所有可能的验证码组合，获取到正确验证码。
- 验证码重放：同一个验证码在使用后未立即失效，可被重复利用多次，攻击者利用此特性配合字典攻击，无限次尝试登录。

③ 账号枚举

定义：由于身份认证机制在处理不存在的用户与存在的用户时，返回了不同的错误信息，或者由于用户标识符（UID）采用了可预测的生成规则，导致攻击者可通过自动化手段探测并收集系统中有效的账号列表。

场景示例：

- 攻击者在登录页面输入一个不存在的账号，系统提示“用户名不存在”，输入一个存在的账号但密码错误，系统提示“密码错误”。
- 系统用户的 UID 是自增的或者有固定规律。

④ 弱口令与默认凭证

定义：系统允许使用极易被猜测的密码，或沿用出厂默认账号密码。

场景示例：用户使用 123456、admin 等常见弱密码，或设备使用厂商预设的默认超级管理员账号。攻击者利用公开的字典进行批量匹配，成功率极高。

2、半数汽车厂商云平台存在过度数据暴露漏洞

在分析的 30 家汽车厂商的云平台中，有 15 家存在过度数据暴露漏洞，占比高达 50.0%。过度数据暴露漏洞是一种常见的 API 漏洞，具有一定的隐蔽性，是造成敏感信息泄露的重要源头。此类漏洞的大面积存在，表明很多汽车厂商在云平台的开发中，存在前后端职责划分不清的问题，后端没有做到严控数据权限，完全依赖于前端应用自行筛选展示所需数据，且在架构设计上没有充分考虑数据安全风险，缺乏必要的安全控制措施，缺失了数据安全防护层，从而导致将关键的数据安全责任，完全寄托于不可控的客户端环境，这违背了最基本的安全原则。

过度数据暴露漏洞（Excessive Data Exposure）

过度数据暴露漏洞是指应用程序后端接口在响应客户端请求时，未遵循“数据最小化”原则，返回了超出当前业务功能所需范围的多余数据，将数据过滤的责任不安全的交给了前端应用，一旦

攻击者通过拦截通信或修改请求等方式直接访问接口，就可能导致大量敏感信息泄露，造成巨大的数据安全风险。

本报告中发现的过度数据暴露类漏洞主要包括：接口响应数据冗余、调试信息与内部结构泄露。

① 接口响应数据冗余

定义： 后端接口在返回数据时，包含了大量与当前业务逻辑无关的字段或关联信息。

场景示例：

- 查询车辆状态时，接口返回了车主手机号、VIN 码、车辆位置等敏感信息。
- 查询用户昵称和头像时，接口返回了完整的用户资料，包括注册时间、最后登录 IP、账户余额、历史订单等。

② 调试信息与内部结构泄露

定义： 系统在错误响应、日志文件或前端代码中，暴露了不应公开的技术细节。

场景示例：

- 错误页面返回详细的堆栈信息，暴露了使用的框架版本、数据库类型、内部类名与方法名。
- 前端 JavaScript 文件中包含未混淆的 API 路径、测试接口地址或硬编码的密钥片段。
- HTTP 响应头中泄露服务器类型、中间件版本。

3、三成汽车厂商云平台存在数字钥匙管理失效漏洞

当前智能网联汽车普遍采用数字钥匙，如蓝牙、UWB、NFC、星闪等。据统计，2025 年 1-8 月中国市场乘用车标配数字钥匙的交付量达到 788.5 万套，搭载率超过 54%，数字钥匙正在从高端选配逐步变为新车标配。

在分析的 30 家汽车厂商云平台中，有 9 家存在数字钥匙管理失效漏洞，占比 30.0%。使用数字钥匙解锁和启动车辆是智能网联汽车专属的核心应用场景，同时也是取得汽车最高控制权限的操作，必须充分考虑安全性。汽车数字钥匙的管理涉及到云平台、车端、移动端等多方协同，攻击面广泛，此类高风险的专属复杂业务场景，尤其需要业务团队和安全团队的紧密合作，从设计阶段就要将安全纳入，并贯穿始终。

数字钥匙管理失效漏洞（Digital Key Management Failures）

数字钥匙管理失效漏洞是指汽车数字钥匙系统在数字钥匙的生命周期管理（包括生成、分发、授权、更新及撤销）过程中，由于机制设计缺陷或安全策略缺失，导致数字钥匙的权限失控，使未授权设备或用户能够非法获取、复制、重放或长期持有车辆控制权。这类漏洞专门针对汽车蓝牙、NFC、UWB 等数字钥匙技术，是汽车网络信息安全领域的专属安全威胁。

本报告中发现的数字钥匙管理失效类漏洞主要包括：数字钥匙非法复制、数字钥匙权限管理失效、数字钥匙授权撤销失败等。

① 数字钥匙非法复制

定义： 系统生成的数字钥匙凭证缺乏硬件绑定或唯一性校验，导致凭证可被提取并复制到其他设备上。

场景示例：攻击者通过物理接触或无线方式提取了合法设备的数字钥匙凭证，并将其写入另一台设备，从而获得与原车主同等的车辆控制权限。

② 数字钥匙权限管理失效

定义：系统在处理数字钥匙的权限分配（如主钥匙、分享钥匙、临时钥匙）时，逻辑存在漏洞，导致权限提升或滥用。

场景示例：被授权者能够通过修改接口参数，生成具有车主权限或无限期有效的数字钥匙，或者二次授权给新的用户。

③ 数字钥匙授权撤销失败

定义：车主通过手机 APP 撤销数字钥匙授权后，被撤销的用户仍能使用数字钥匙解锁和启动车辆。

场景示例：服务器端撤销指令未同步到车辆 ECU，或者撤销操作存在时间窗口，攻击者在此期间仍可操作。

四、主要漏洞危害分析

经过真实车辆验证发现，在汽车厂商云平台中发现的漏洞主要可造成远程解锁车辆、近场解锁车辆、未授权驾驶车辆、敏感信息泄露、远程影响 OTA、冒用账户进行未授权操作、远程控制服务器等多种危

害。漏洞造成的各种危害及影响的汽车厂商数量和占比如下表所示。

危害类型	影响厂商数量	影响厂商数量占比
敏感信息泄露	22	73.3%
远程解锁车辆	18	60.0%
未授权驾驶车辆	13	43.3%
冒用账户进行未授权操作	12	40.0%
近场解锁车辆	9	30.0%
远程影响 OTA	2	6.7%
远程控制服务器	1	3.3%

1、 超七成汽车厂商云平台存在敏感信息泄露，数据安全风险突出

在分析的 30 家汽车厂商云平台中，有 22 家存在因漏洞导致的敏感信息泄露问题，占比高达 73.3%，整体数据安全风险非常突出。这些云平台的敏感信息泄漏问题由多类漏洞引发，包括过度数据暴露、失效的访问控制、身份认证失效、会话管理失效等。泄露的敏感信息涵盖多种类型，包括姓名、性别、手机号、生日、邮箱、账户资产、IP 地址、收货地址等用户相关信息，车牌号、车辆型号、车辆 VIN 码、车身颜色、车辆实时位置、泊车周边环境等车辆相关信息。

例如，某汽车厂商 A 的云平台中存在 1 个过度数据暴露漏洞（接口响应数据冗余）和 2 个失效的访问控制漏洞（越权访问），组合利用这 3 个漏洞，该厂商 APP 的任意注册用户均可通过其云平台数据接

口批量获取真实车主及相关车辆的敏感信息，包括手机号、用户 id、部分真实姓名、车辆 VIN 码和实时位置等。某汽车厂商 B 的云平台中存在 1 个身份认证失效漏洞（账号枚举）和 1 个失效的访问控制漏洞（越权访问），组合利用这 2 个漏洞，该厂商 APP 的任意注册用户均可通过其云平台数据接口批量获取真实车主及相关车辆的敏感信息，包括姓名、性别、用户 id、手机号、邮箱、车辆 VIN 码、车身颜色和实时位置等。

攻击者可利用这些漏洞组合实施大规模数据窃取，严重危害车企的数据安全。窃取的数据还可帮助攻击者进行“精准攻击”，例如攻击者可通过被攻击目标的手机号，锁定车辆实时位置，进而实施诈骗、安装窃听装置等违法犯罪活动，严重危害车主人身和财产安全。如果再结合远程或近场解锁车辆的漏洞进行攻击，则会造成更大的危害。

2、2/3 厂商的汽车可利用漏洞在未授权情况下解锁，直接危害车辆财产安全

在分析的 30 家汽车厂商中，有 20 家存在可利用漏洞在未授权情况下远程或近场解锁车辆的问题，占比高达 66.7%，其中 13 家在未授权解锁后，可直接启动和驾驶车辆，占比高达 43.3%。未授权解锁车辆的问题由多类漏洞引发，包括失效的访问控制、身份认证失效、数字钥匙管理失效、会话管理失效、业务逻辑漏洞等。攻击者可以利用漏洞在车主未授权的情况下解锁车辆，并将车辆开走，就像家里的防盗门锁可以被盗贼轻易打开并取走财物一样，毫无安全性可言。

例如，某汽车厂商 B 的云平台中存在 1 个失效的访问控制漏洞（越权访问），系统没有对发起控车指令的用户身份和目标车辆进行有效的绑定校验，导致其 APP 任意注册用户只需获知目标车辆 VIN 码，即可绕过权限限制，远程解锁并启动车辆。车辆 VIN 码通常位于车辆前挡风玻璃下方，停车时从车外清晰可见，极易获取，因此该漏洞的攻击门槛极低，使得车辆的锁车状态几乎形同虚设。前述分析提到，该厂商 B 还存在敏感信息泄漏的问题，攻击者可以利用漏洞组合批量获取到该厂商汽车的 VIN 码、车辆实时位置，这两者结合起来，攻击者就可以使用自动化脚本对该厂商汽车进行批量定位、解锁和启动，造成大规模的车辆资产风险。

某汽车厂商 C 的云平台中存在 1 个数字钥匙管理失效漏洞（数字钥匙授权撤销失败），其云平台、车端和移动端的数字钥匙授权未能有效同步，导致即使车主主动取消了被授权者账号的控车权限，该被授权者仍能使用手机近场解锁、启动和驾驶车辆。在租车或借车场景下，此类漏洞会导致“临时钥匙”变成“永久钥匙”，直接危害用户的车辆财产安全，并可能因此引发一系列其他严重的安全问题。

3、四成汽车厂商云平台存在用户账户被冒用进行未授权操作的安全风险

在分析的 30 家汽车厂商云平台中，有 12 家存在可利用漏洞冒用用户账户进行未授权操作的问题，占比 40.0%。冒用用户账户进行未授权操作的问题由多类漏洞引发，包括失效的访问控制、身份认证失

效、会话管理失效等。此类问题在不同厂商的云平台中表现各不相同，一些经过验证的典型危害场景和影响包括：（1）直接盗用账户内余额完成充电等消费操作，造成用户的财产损失；（2）攻击者借助冒用的账户，为任意手机号预约经销商试驾服务，占用正常用户的服务资源，扰乱经销商的试驾预约秩序；（3）针对车主账户的冒用，攻击者可篡改车辆授权账号的有效时间，或提升授权权限，直接威胁车辆财产安全；（4）攻击者可删除车辆电子围栏设置，解除安全边界告警，增加车辆被盗风险；（5）打开或关闭车辆的行程统计功能，可能泄露车主的出行轨迹、生活习惯等隐私信息。

五、总结及建议

智能网联汽车的网络信息安全是一个极其复杂的系统性工程，本报告中只分析了云平台本身的安全性，且因分析条件和时间等因素的限制，对 30 家汽车厂商云平台的漏洞分析并不足够完善和深入，仅是管中窥豹。但即便如此，分析所发现的问题已经极其严重，大量基础性漏洞的普遍存在，揭示的是体系化的缺失：安全主体责任未能落实，产品安全研发基础薄弱，车云协同防御链条断裂。

综上，我们建议智能网联汽车厂商：

1、提升战略高度，压实安全主体责任

网络信息安全是智能网联汽车的生命线，必须从企业战略层面予以高度重视。

建议一：将网络信息安全上升为“一把手工程”，明确企业主要

负责人为网络信息安全第一责任人。设立专门的安全管理机构，统筹和落实网络信息安全工作，设立年度网络信息安全专项预算，确保安全投入不低于信息化总投入的一定比例，为安全体系建设提供持续的资金与资源保障。

2、践行内生安全，筑牢产品研发根基

将安全能力内生于产品研发全生命周期，在产品出厂前就植入安全基因，解决“先天不足”的问题。

建议二：推行安全开发生命周期，将安全需求分析、威胁建模、代码审计、渗透测试等环节强制嵌入产品开发流程，从源头削减漏洞数量。

建议三：强化软件供应链安全管控，建立软件物料清单（SBOM）管理机制，对供应商软件、开源组件进行严格的安全把关，并进行持续的漏洞监测与修复。

建议四：建立产品漏洞响应机制，包括漏洞报告接收、评估定级、处置修复等；设立公开的漏洞奖励计划，借助外部研究力量持续发现漏洞；推行常态化、实战化安全验证，每年至少对云端和车端的核心功能及新功能进行一次深度白盒渗透测试，以攻促防。

3、深化车云协同，构建主动免疫体系

依托车云协同，打造具备自我感知、自我防御、自我进化能力的主动免疫安全体系，实现从“单点防御”到“体系化防控”的跨越。

建议五：实施零信任架构，重构访问控制体系。部署基于身份的动态细粒度访问控制网关，无缝集成至车云业务环境，实现 API 接口

的统一、安全管控。对每一次来自车辆、移动端或业务平台管理端的请求进行持续验证和最小权限授权，确保敏感操作和敏感数据仅在强认证与强授权下被执行和访问。

建议六：强化应用层深度防御，引入运行时应用自保护（RASP）技术，将保护引擎嵌入到云应用内部，实时监测和阻断异常行为，从内部防御漏洞攻击。

建议七：建立统一身份与密钥管理中心，对车联网场景下所有车辆、用户、设备的海量数字身份与密钥实施集中化管理，实现密钥全生命周期的自动化发放、轮转、吊销与审计闭环管控。

建议八：落实数据分类分级保护，依据法律法规对数据进行分类分级，针对不同的数据，实施差异化的安全策略，包括数据加密存储、传输加密、脱敏处理以及严格的访问权限控制，确保数据全生命周期的安全合规。

建议九：建立车端主动防御机制，在车端关键节点部署轻量级入侵检测与防护系统（IDPS），实时监控车内网络（CAN、以太网）流量与系统进程，具备深度报文解析与异常行为建模能力，可精准识别并阻断攻击行为。

建议十：建设车云协同安全运营平台（AISOC），集中汇总云端安全事件、车端 IDPS 告警、威胁情报等多源数据，利用 AI 进行关联分析，实现安全威胁的“全局可见、精准研判、协同响应”。一旦云端发现新型攻击，可即时将防御特征下发至全网车辆，做到“分钟级”的全局免疫，真正实现“云脑”指挥“端手”的闭环运营。

附录：奇安信代码安全实验室简介

奇安信代码安全实验室是奇安信集团旗下，专注于软件源代码安全分析技术、二进制漏洞挖掘技术研究与开发的团队。实验室支撑国家级漏洞平台的技术工作，多次向国家信息安全漏洞库（CNNVD）、国家信息安全漏洞共享平台（CNVD）、工信部网络安全威胁和漏洞信息共享平台(NVDB)等报送原创通用型漏洞信息并获得表彰；帮助微软、谷歌、苹果、Cisco、Juniper、Red Hat、Ubuntu、Oracle、Adobe、VMware、阿里云、飞塔、华为、施耐德、Mikrotik、Netgear、D-Link、Netis、ThinkPHP、以太坊、Facebook、亚马逊、IBM、SAP、NetFlix、Kubernetes、Apache 基金会、腾讯、滴滴等大型厂商和机构的商用产品或开源项目发现了千余个安全缺陷和漏洞，并获得公开致谢。目前，实验室拥有国家信息安全漏洞库（CNNVD）特聘专家一名，工信部汽车漏洞库（NVDB-CAVD）特聘专家一名，多名成员入选微软全球 TOP 安全研究者、Oracle 安全纵深防御计划贡献者等精英榜单。在 Pwn2Own 2017 世界黑客大赛上，实验室成员还曾获得 Master of Pwn 破解大师冠军称号。

奇车安全是奇安信代码安全实验室负责智能网联汽车安全研究的团队，对主流智能网联汽车产品进行了大量的安全研究工作，在 30 多个汽车品牌的产品中发现了数百个安全漏洞，并曾获得 2025 工信部 NVDB-CAVD 春季汽车信息安全挑战赛第一名、中国计算机学会(CCF)首届汽车安全攻防大赛一等奖、赛力斯问界首届汽车安全大赛冠军等

多个奖项。

基于奇安信代码安全实验室多年的技术积累，奇安信集团在国内率先推出了自主可控的软件代码安全分析系统——奇安信代码卫士和奇安信开源卫士。

奇安信代码卫士是一款高度可扩展的静态应用程序安全测试系统，该系统提供了一套企业级源代码缺陷分析、源代码合规分析、IaC 安全分析的解决方案，在不改变企业现有开发测试流程的前提下，与软件版本管理、持续集成、缺陷跟踪等系统进行集成，将源代码安全分析融入企业开发测试流程中，实现软件源代码安全目标的统一管理、自动化检测、差距分析、缺陷修复追踪等功能，帮助企业以最小代价建立代码安全保障体系并落地实施，构筑信息系统的“内建安全”。奇安信代码卫士目前支持 C、C++、C#、Objective-C、Swift、Java、PHP、Python、Cobol、Go 等 32 种编程语言，可检测 3500 多种源代码安全缺陷，支持多个国际、国内主流标准和规范的检测。

奇安信开源卫士是一款集开源软件识别与安全管控于一体的软件成分分析系统，该系统通过智能化数据收集引擎在全球范围内获取开源软件基础信息、协议信息及其相关漏洞信息，利用自主研发的开源软件分析引擎为企业提供开源软件资产识别、开源软件漏洞风险分析、开源软件协议风险分析、开源软件运维风险分析、开源软件漏洞情报预警及开源软件安全管理等功能，帮助企业掌握开源软件资产信息及相关风险，及时获取最新开源软件漏洞情报，降低由开源软件给企业带来的风险，保障企业交付更安全的软件。奇安信开源卫士目前

支持超过 2.3 亿开源软件版本的识别，支持源代码、二进制、容器镜像、操作系统的开源软件成分分析，兼容 NVD、CNNVD、CNVD 等多种漏洞情报来源。奇安信代码卫士和奇安信开源卫士已经在近千家大型机构和企业中应用，入选国家发改委数字化转型伙伴行动、工信部中小企业数字化赋能专项行动，为中小企业提供软件代码安全检测平台和服务。