奇安信
新一代网络安全领军者

Apache Flink 高危漏洞

安全风险通告

奇安信 CERT

2021 年 01 月 06 日

目录

第1章 安全通告

尊敬的客户：

Flink 核心是一个流式的数据流执行引擎，其针对数据流的分布式计算提供了数据分布、数据通信以及容错机制等功能。Flink 1.5.1 引入了 REST API ，但其实现上存在多处缺陷。2021 年 1 月 5 日，Apache Flink 官方发布安全更新，修复了 2 个高危漏洞：CVE-2020-17519：攻击者可通过 JobManager 进程的 REST 接口配合../进行目录跳转实现系统任意文件读取；CVE-2020-17518：通过 REST API 并结合../进行目录跳转，可实现任意文件上传，覆盖系统文件。

奇安信 CERT 将持续关注该漏洞进展，并第一时间为您更新该漏洞信息。

第2章 文档信息

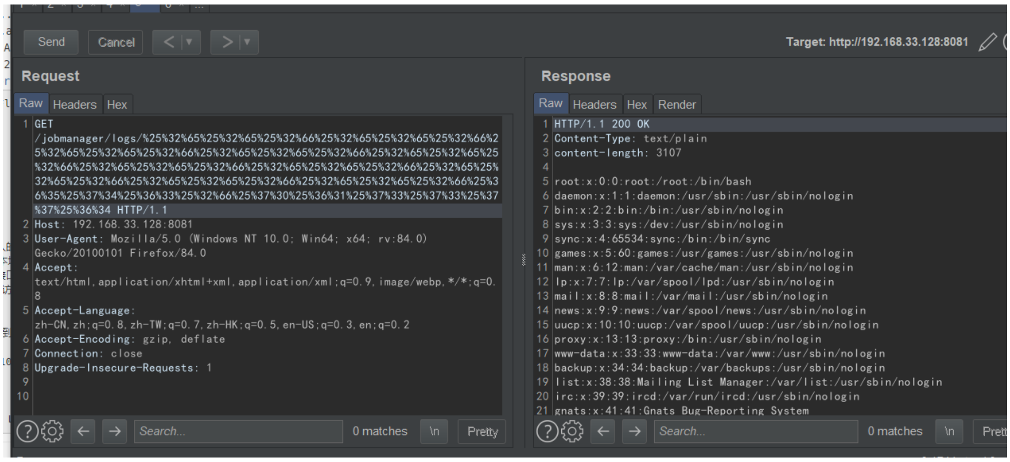
文档名称	Apache Flink 高危漏洞安全风险通告
关键字	任意文件读取、任意文件上传
发布日期	2021 年 01 月 06 日
分析团队	奇安信 CERT

第3章 漏洞信息

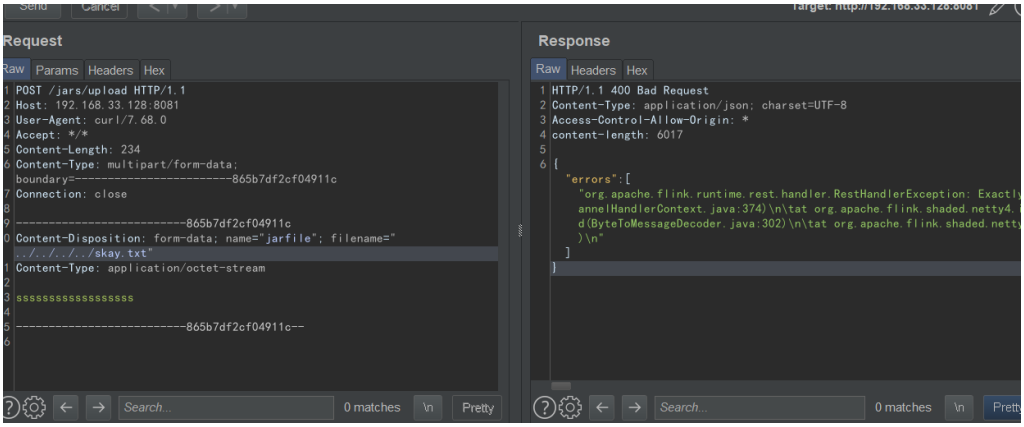
3.1 漏洞描述

2021 年 1 月 5 日，Apache 官网发布公告，通报了 Apache Flink 两个高危漏洞，漏洞触发点均为 REST API 接口。Flink 1.5.1 引入了 REST API ，但其存在多处缺陷。

CVE-2020-17519，利用 JobManager 进程的 REST 接口，配合../进行目录跳转进行系统任意文件读取，成功利用需要../进行两次 url 编码，值得注意的是此功能接口为 Apache Flink 1.11.0 中引入的一项更改（并在 1.11.1 和更高版本中发布）复现截图如下：



CVE-2020-17518，通过 REST API，配合../进行目录跳转，可实现上传文件到目标系统任意位置，进一步利用可覆盖系统敏感文件，获取目标控制权限，复现截图如下:



3.2 风险等级

奇安信 CERT 风险评级为：高危

风险等级：蓝色（一般事件）

第4章 影响范围

CVE-2020-17518: 1.5.1 <= Apache Flink <= 1.11.2

CVE-2020-17519: Apache Flink 1.11.0、1.11.1、1.11.2

第5章 处置建议

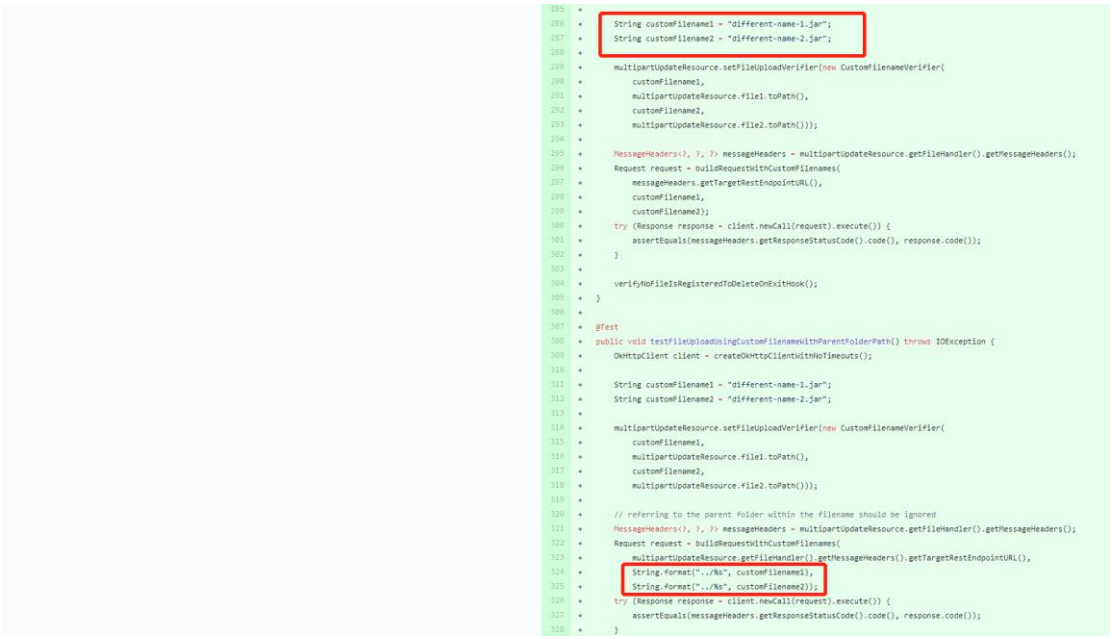
建议受影响的用户将 Flink 升级到 1.11.3 或 1.12.0

下载地址：https://flink.apache.org/downloads.html

第6章 技术分析

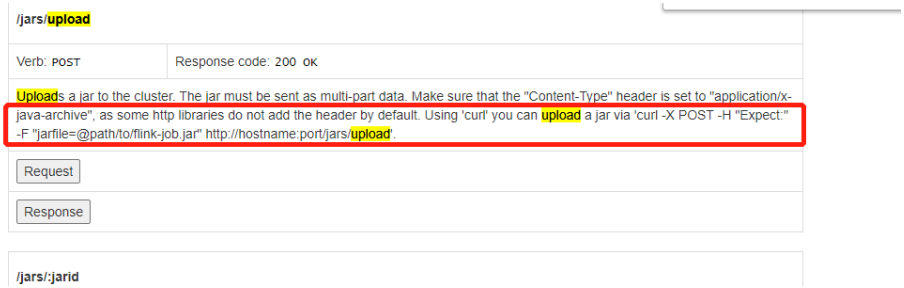
CVE-2020-17518 根据官方通告，我们定位到 commit :a5264a6f41524afe8ceadf1d8ddc8c80f323ebc4，https://github.com/apache/flink/commit/a5264a6f41524afe8ceadf1d8ddc8c80f323ebc4，

FileUploadHandlerTest.java 中有如下信息：



```
+    String customFilename1 = "different-name-1.jar";
+    String customFilename2 = "different-name-2.jar";
+
+    multipartUpdateResource.setFileUploadVerifier(new CustomFilenameVerifier(
+        customFilename1,
+        multipartUpdateResource.file1.toPath(),
+        customFilename2,
+        multipartUpdateResource.file2.toPath()));
+
+    MessageHeaders<?, ?, ?> messageHeaders = multipartUpdateResource.getFileHandler().getMessageHeaders();
+    Request request = buildRequestWithCustomFilenames(
+        messageHeaders.getTargetRestEndpointURL(),
+        customFilename1,
+        customFilename2);
+    try (Response response = client.newCall(request).execute()) {
+        assertEquals(messageHeaders.getResponseStatusCode().code(), response.code());
+    }
+
+    verifyNoFileIsRegisteredToDeleteOnExitHook();
+}
+
+@Test
+public void testFileUploadUsingCustomFilenameWithParentFolderPath() throws IOException {
+    OkHttpClient client = createOkHttpClientWithNoTimeouts();
+
+    String customFilename1 = "different-name-1.jar";
+    String customFilename2 = "different-name-2.jar";
+
+    multipartUpdateResource.setFileUploadVerifier(new CustomFilenameVerifier(
+        customFilename1,
+        multipartUpdateResource.file1.toPath(),
+        customFilename2,
+        multipartUpdateResource.file2.toPath()));
+
+    // referring to the parent folder within the filename should be ignored
+    MessageHeaders<?, ?, ?> messageHeaders = multipartUpdateResource.getFileHandler().getMessageHeaders();
+    Request request = buildRequestWithCustomFilenames(
+        multipartUpdateResource.getFileHandler().getMessageHeaders().getTargetRestEndpointURL(),
+        String.format("../%s", customFilename1),
+        String.format("../%s", customFilename2));
+    try (Response response = client.newCall(request).execute()) {
+        assertEquals(messageHeaders.getResponseStatusCode().code(), response.code());
+    }
```

结合官方通告中指出的 REST API，查阅官方文档，https://ci.apache.org/projects/flink/flink-docs-release-1.11/monitoring/rest_api.html 定位到文件上传功能



/jars/upload

Verb: POST | Response code: 200 OK

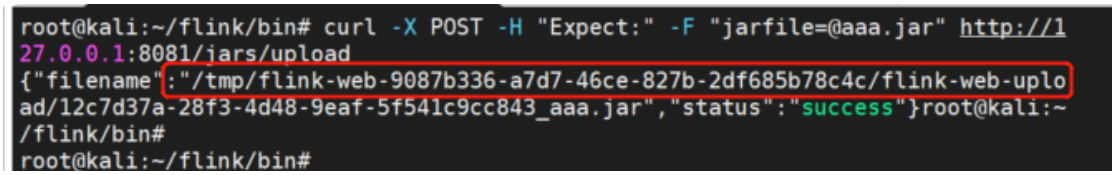
Uploads a jar to the cluster. The jar must be sent as multi-part data. Make sure that the "Content-Type" header is set to "application/x-java-archive", as some http libraries do not add the header by default. Using 'curl' you can upload a jar via 'curl -X POST -H "Expect:" -F "jarfile=@path/to/flink-job.jar" http://hostname:port/jars/upload'.

Request

Response

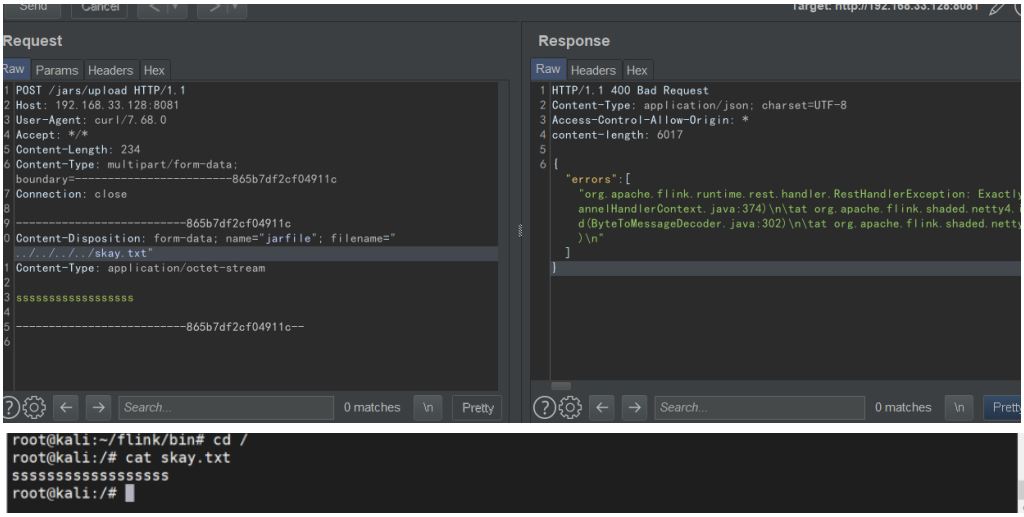
/jars/:jarid

构造 curl 上传请求成功将文件上传至系统指定 tmp 目录下

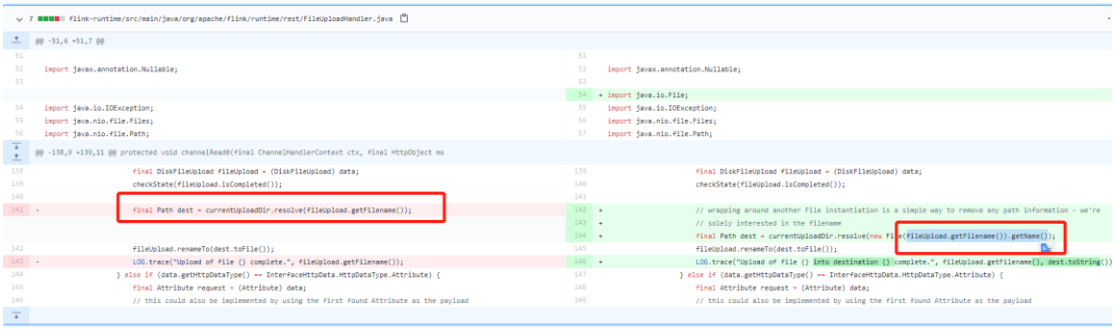


```
root@kali:~/flink/bin# curl -X POST -H "Expect:" -F "jarfile=@aaa.jar" http://127.0.0.1:8081/jars/upload
{"filename":"/tmp/flink-web-9087b336-a7d7-46ce-827b-2df685b78c4c/flink-web-upload/12c7d37a-28f3-4d48-9eaf-5f541c9cc843_aaa.jar","status":"success"}root@kali:~/flink/bin#
root@kali:~/flink/bin#
```

Burp 拦截 curl 请求，修改文件名进行目录上传跳转

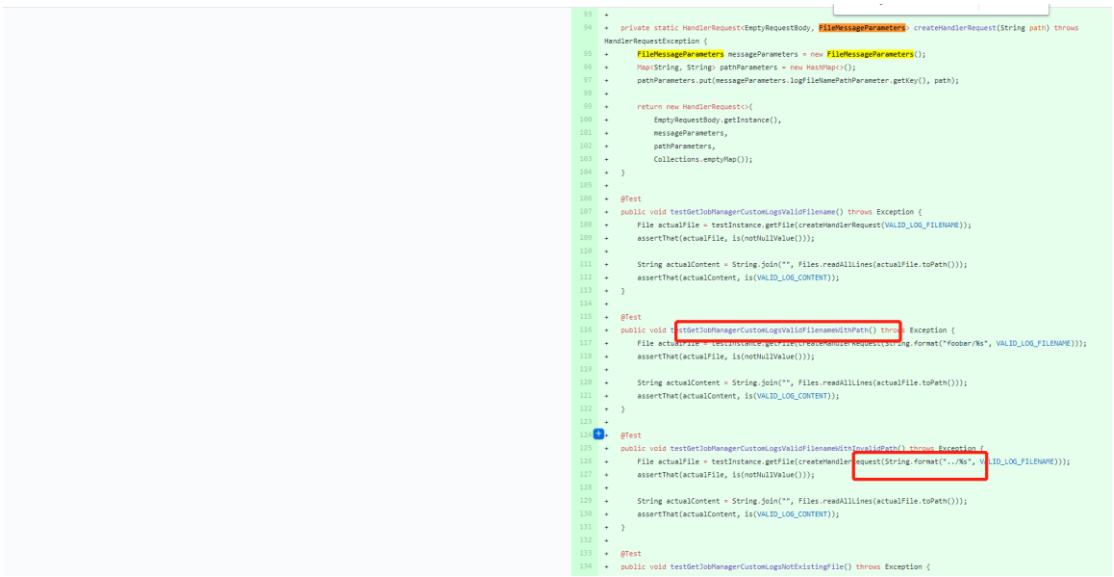


成功上传至根目录，代码中 Flink 并没有对上传文件名进行有效处理，官方修复为增加了 fileUpload.getFilename().getName()，使跳目录无效。

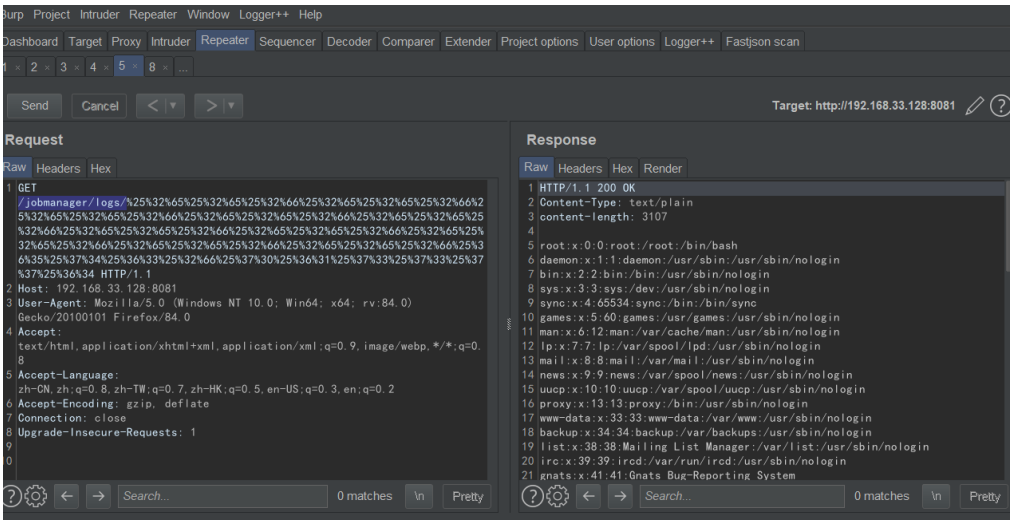


还可覆盖系统原有文件进行更进一步利用。

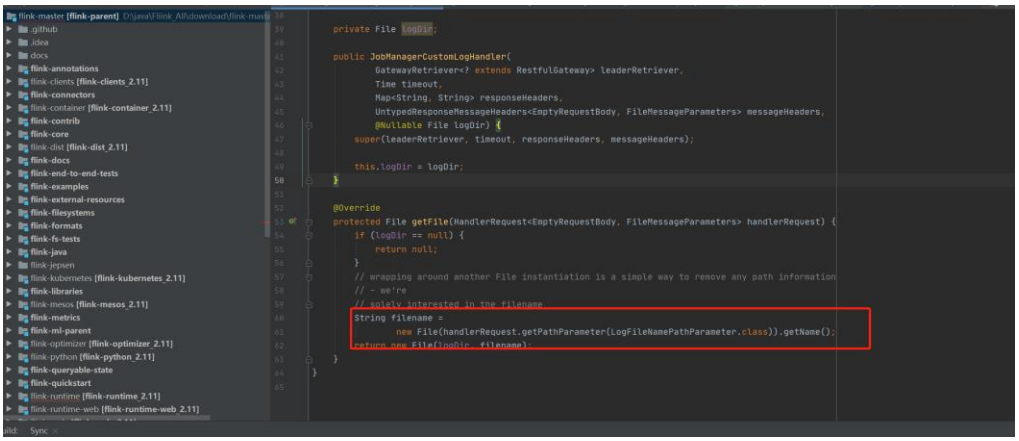
CVE-2020-17519 根据官方通告，我们定位到 https://github.com/apache/flink/commit/b561010b0ee741543c3953306037f00d7a9f0801



根据方法名称 testGetJobManagerCustomLogsValidFilename，去官方文档中查找 GetJobManager log 相关功能，定位到/jobmanager/logs/ API 接口，值得注意一点，由于 Flink 会根据“/”进行路由判断，直接../进行目录跳转无效，需要将 payload 进行二次 url 编码



官方修复同文件上传一样，JobManagerCustomLogHandler.java 中，在获取了文件名后又增加了 getName()



第7章 产品解决方案

7.1 奇安信开源卫士已更新

奇安信开源卫士 20210106. 553 版本已支持对 Apache Flink 任意文件读取漏洞（CVE-2020-17519）以及 Apache Flink 任意文件上传漏洞（CVE-2020-17518）的检测。

7.2 奇安信天眼产品解决方案

奇安信天眼新一代威胁感知系统在第一时间加入了该漏洞的检测规则，请将规则包升级到 3.0.0106.12568 及以上版本。规则名称：Apache Flink 任意文件上传漏洞(CVE-2020-17518)，规则 ID：0x10020BA1；规则名称：Apache Flink 任意文件读取漏洞(CVE-2020-17519)，规则 ID：0x10020BA2；。奇安信天眼流量探针（传感器）升级方法：系统配置->设备升级->规则升级，选择“网络升级”或“本地升级”。

7.3 奇安信网神网络数据传感器系统产品检测方案

奇安信网神网络数据传感器（NDS3000/5000/9000 系列）产品，已具备该漏洞的检测能力。规则 ID 为：6129，建议用户尽快升级检测规则库至 2101061400 以后版本并启用该检测规则。

7.4 奇安信网神智慧防火墙产品防护方案

奇安信新一代智慧防火墙（NSG3000/5000/7000/9000 系列）和下一代极速防火墙（NSG3500/5500/7500/9500 系列）产品系列，已通过更新 IPS 特征库完成了对该漏洞的防护。建议用户尽快将 IPS 特征库升级至”2101061300”及以上版本并启用规则 ID: 1232201、1232101 进行检测。

7.5 奇安信网站应用安全云防护系统已更新防护特征库

奇安信网神网站应用安全云防护系统已全局更新所有云端防护节点的防护规则，支持对 Apache Flink 高危漏洞(CVE-2020-17518/CVE-2020-17519)的防护。

7.6 奇安信网神统一服务器安全管理平台更新入侵防御规则库

奇安信网神虚拟化安全轻代理版本可通过更新入侵防御规则库 2021.01.12 版本，支持对 Apache Flink 高危漏洞 CVE-2020-17519：任意文件读取 CVE-2020-17518 任意文件上传防护，当前规则正在测试中，将于 1 月 12 日发布，届时请用户联系技术支持人员获取规则升级包对轻代理版本进行升级。

奇安信网神统一服务器安全管理平台可通过更新入侵防御规则库 10322 版本，支持对 Apache Flink 高危漏洞 CVE-2020-17519：任意文件读取 CVE-2020-17518 任意文件上传的防护，当前规则正在测试中，将于 1 月 12 日发布，届时请用户联系技术支持人员获取规则升级包对融合版本进行升级。

7.7 奇安信开源卫士已更新

奇安信开源卫士 20210106. 553 版本已支持对 Apache Flink 任意文件读取漏洞（CVE-2020-17519）以及 Apache Flink 任意文件上传漏洞（CVE-2020-17518）的检测。

第8章 参考资料

[1] https://lists.apache.org/thread.html/rb43cd476419a48be89c1339b527a18116f23eec5b6df2b2acbfef261%40%3Cdev.flink.apache.org%3E

[2] https://lists.apache.org/thread.html/r6843202556a6d0bce9607ebc02e303f68fc88e9038235598bde3b50d%40%3Cdev.flink.apache.org%3E

奇安信 CERT

【我们是谁】

奇安信应急响应部（又称：奇安信 CERT，奇安信 A-TEAM）成立于 2016 年，是属于奇安信旗下的网络安全应急响应平台，平台旨在第一时间为客户提供漏洞或网络安全事件安全风险通告、响应处置建议、相关技术和奇安信相关产品的解决方案。

奇安信 A-TEAM：团队主要致力于 Web 渗透、APT 攻防、对抗，前瞻性攻防工具预研。从底层原理、协议层面进行严肃、有深度的技术研究，深入还原攻与防的技术本质，曾多次率先披露 Windows 域、Exchange、WebLogic、Exim 等重大安全漏洞，第一时间发布相关漏洞风险通告及可行的处置措施并获得官方致谢。欢迎有意者加入！

【我们的服务】

安全风险通告：奇安信 CERT 成立至今已发布上百篇安全风险通告，从成立至今，针对多个高危漏洞、网络安全事件发布风险通告并给出了有效的安全措施。我们的安全研究团队将实时跟踪安全热点事件和漏洞，始终站在用户的视角去评估风险，致力于第一时间向客户发送有效的风险和相关解决方案。

【订阅方式】

发送接收邮箱和所属单位至：

cert@qianxin.com

【微信公众号】

奇安信 CERT