ICS 33.050
CCS M 30

团 体 标 准

T/TAF 166—2023

漏洞补丁验证通用方法

Common method for verifying vulnerability patches

2023-04-26 发布

2023-04-26 实施

电信终端产业协会 发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件中的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、启明星辰信息技术集团股份有限公司、郑州信大捷安信息技术股份有限公司、武汉网锐检测科技有限公司、成都泰瑞通信设备检测有限公司、上海泰峰检测认证有限公司、中兴通讯股份有限公司、联想（北京）有限公司、华为技术有限公司、新华三技术有限公司、西安通和电信设备检测有限公司、博鼎实华(北京)技术有限公司。

本文件主要起草人：刘欣东、吴荣春、丁斌、王伟、刘为华、康亮、陈玺、龚志红、吴翔宇、宋祥烈、周继华、刘俊、叶郁柏、童天予、赵艳峰、刘雅闻、张亚薇、刘向东。

引　言

随着网络规模的不断扩大，我国网络设备、操作系统、第三方组件等漏洞频发，需要及时对漏洞进行补丁升级，当完成漏洞补丁升级后如何对漏洞补丁自身的安全性和其有效性进行验证成为电信、电力、金融等各行业高度关注的重要问题。为规范漏洞补丁的验证方法，提高漏洞补丁的安全性、有效性，支撑相关企业开展漏洞补丁的全周期管理和验证，依据《中国人民共和国网络安全法》、《网络产品安全漏洞管理规定》等相关法律法规，提出本文件。

漏洞补丁验证通用方法

1 范围

本文件规定了漏洞补丁的通用验证方法，主要从漏洞补丁验证流程、漏洞补丁测试环境、漏洞补丁验证方法等方面作了要求。

本文件适用于针对漏洞补丁开展验证工作，旨在向漏洞补丁使用人员和验证人员提供通用的漏洞补丁验证方法，还可用于指导漏洞补丁的测试、发布工作。

注：验证漏洞补丁类型可以是网络产品和服务提供者或使用者的漏洞补丁、操作系统漏洞补丁、应用程序漏洞补丁和开源软件漏洞补丁等软件。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 40050—2021 网络关键设备安全通用要求

GB/T 25069 信息安全技术 术语

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

GB/T 30276—2020 信息安全技术 网络安全漏洞管理规范

3 术语和定义

GB/T 25069 中界定的以及下列术语和定义适用于本文件。

3.1

用户 user

使用网络产品和服务的个人或组织。

3.2

网络产品和服务提供者 provider of network product and services

提供网络产品和服务的个人或组织。

3.3

漏洞 vulnerability

可能被威胁利用的资产或控制的弱点。

[来源：GB 40050—2021，3.3]

3.4

有效性 effectiveness

完成修复或达到修复结果的安全程度。

3.5

漏洞发现 vulnerability discovery

通过技术手段，识别出网络产品和服务存在漏洞的过程。

4 缩略语

下列缩略语适用于本文件。

EXP：漏洞利用（Exploit）

POC：概念验证（Proof of Concept）

5 漏洞补丁验证流程

漏洞补丁验证的过程分为接收、准备、验证、发布四个阶段。

a) 接收：

接收阶段是由网络产品和服务提供者向验证人员提供漏洞补丁及其说明材料（见附录B）。

b) 准备：

准备阶段主要是制定漏洞补丁验证的策略，包括确定漏洞验证的方法，进行人员和工具的筹备工作。

在接收漏洞补丁之后，对漏洞补丁及说明材料进行分析，确定产品中存在的问题。

对漏洞进行技术分析，根据漏洞威胁状态，包括POC/EXP状态和已公开的技术细节状态，确定漏洞补丁验证的方法，漏洞补丁验证方法包括：完整性验证、标识唯一性验证、恶意代码检查、安装验证、一致性验证和动态验证。

c) 验证：

搭建验证环境，根据确定的漏洞补丁验证的策略，对漏洞补丁进行验证，记录验证结果。

d) 发布：

将验证结果通知提供者，正式发布漏洞补丁验证结果。

漏洞补丁验证流程如图1所示：

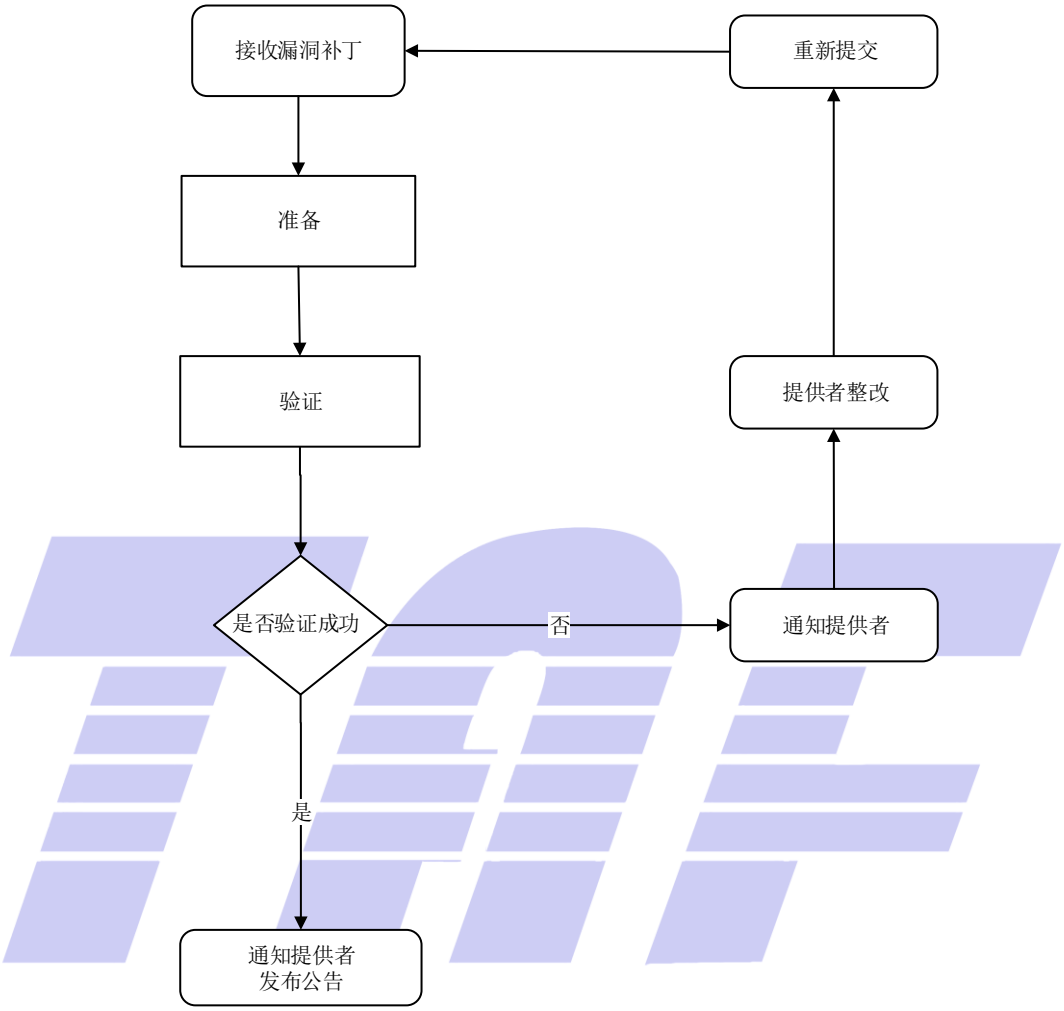

图1　漏洞补丁验证流程

6　验证环境

验证环境如图 2 所示。

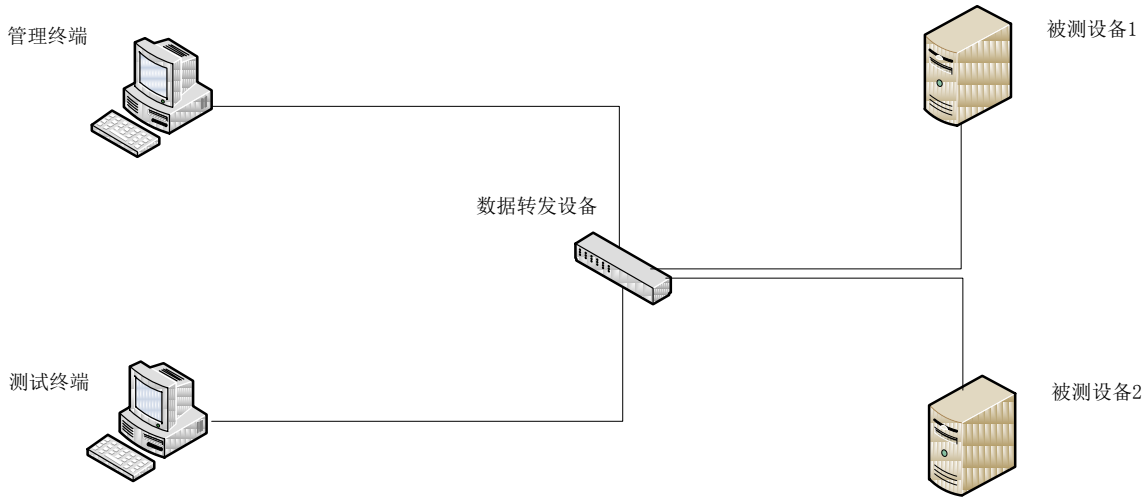

图 2　漏洞补丁验证环境

被测设备 1，部署修补前的网络设备环境、操作系统环境和应用程序环境。

被测设备 2，部署修补后的网络设备环境、操作系统环境和应用程序环境。

管理终端，一般连接到被测设备的管理接口，用于对被测设备进行配置管理。

测试终端，一般连接到设备的业务接口或管理接口，用于发送网络数据包、工业控制数据包等数据，进行漏洞补丁验证。

数据转发设备用于连接管理终端、测试终端与被测设备，实现网络数据或工业控制数据的互通。

7　漏洞补丁验证方法

7.1　漏洞补丁完整性验证

该评估项包括如下内容：

a）　安全要求：

漏洞补丁包/升级包的完整性、来源真实性应与提供的说明材料一致。

b）　预置条件：

1）　漏洞补丁提供者提供说明材料或自验证证明材料，提供对漏洞补丁包/升级包的完整性、来源真实性进行验证的方法。

2）　漏洞补丁包/升级包中包含为用户提供的漏洞补丁包/升级包的完整性信息。

c）　检测方法：

1）　检查漏洞补丁提供者提供的说明材料，确认是否包含为用户提供的对漏洞补丁包/升级包的完整性、来源真实性进行验证的方法。

2）　检查漏洞补丁包/升级包是否包含为用户提供的漏洞补丁包/升级包的完整性信息。

3）　参照漏洞补丁提供者提供的说明材料，对漏洞补丁包/升级包的完整性、来源真实性进行验证。

d）　预期结果：

1）　说明材料中明确包含为用户提供的对漏洞补丁包/升级包的完整性、来源真实性进行验证

的方法。

2） 漏洞补丁包/升级包中包含为用户提供的漏洞补丁包/升级包的完整性信息。

3） 漏洞补丁包/升级包的完整性信息与说明材料中提供的结果一致。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.2 漏洞补丁标识唯一性验证

该评估项包括如下内容：

a） 安全要求：

漏洞补丁应具备唯一性标识，应采用结构化命名方式。

b） 预置条件：

漏洞补丁提供者提供说明材料或自验证证明材料，包括预装软件、漏洞补丁包/升级包的唯一性标识方式、版本号等。

c） 检测方法：

1） 检查漏洞补丁包/升级包的不同版本唯一性标识；

2） 漏洞补丁标识命名采取结构化命名方式，至少包含产品类型、版本等要素。

d） 预期结果：

1） 漏洞补丁包/升级包具备唯一性标识；

2） 漏洞补丁包/升级包标识采取结构化命名方式。

e） 判定原则：

1） 测试结果应与预期结果相符，否则不符合要求；

2） 漏洞补丁包/升级包唯一性标识可以是分配的唯一版本号、软件哈希值等标识信息中的一个或多个。

7.3 漏洞补丁恶意程序检测

该评估项包括如下内容：

a） 安全要求：

漏洞补丁包/升级包不应存在恶意程序。

b） 预置条件：

漏洞补丁提供者提供的漏洞补丁包/升级包。

c） 检测方法：

使用至少两种恶意程序检查工具对漏洞补丁包/升级包进行文件检查。

d） 预期结果：

漏洞补丁包/升级包未发现恶意程序。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.4 漏洞补丁安装验证

该评估项包括如下内容：

a） 安全要求：

漏洞补丁包/升级包应能够成功安装。安装后系统和应用服务应能够正常启动。

b） 预置条件：

漏洞补丁提供者提供漏洞补丁包/升级包及其说明材料或自验证证明材料，并提供安装补丁所

需的硬件设备、操作系统和应用程序，说明材料中包含漏洞补丁相关硬件设备、操作系统、应用程序和补丁的部署方法和配置管理方法，提供漏洞补丁验证所需的系统、服务账户口令信息。

c) 检测方法：

1) 参照说明材料，对漏洞补丁包/升级包进行安装验证；

2) 漏洞补丁安装过程中是否正确无误，安装后系统能否正常启动，应用服务是否正常启动。

d) 预期结果：

漏洞补丁包/升级包可成功安装。安装后系统能够正常启动，应用服务能够正常启动。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.5 漏洞补丁一致性验证

根据对相关漏洞的分析结果，进行漏洞补丁一致性验证。参照厂商提供的漏洞修补说明，对升级前后的文件进行检查分析，确认漏洞补丁实际修补内容与漏洞修补说明的一致性。具体分析方法参考附录A。

该评估项包括如下内容：

a) 安全要求：

漏洞补丁实际修补内容应与漏洞修补说明一致。

b) 预置条件：

漏洞补丁提供者提供说明材料或自验证证明材料，说明材料中包含漏洞补丁包/升级包的修改说明，包括修补的安全缺陷、漏洞等安全问题、修改的文件及其路径、修改内容、存在漏洞文件版本号、修复漏洞补丁文件版本号、记录的日志信息。记录漏洞补丁相关漏洞信息，信息内容参见附录表B.1。

c) 检测方法：

1) 检查漏洞补丁提供者提供的说明材料，确认是否包含漏洞补丁包/升级包修改说明，包括修补的安全缺陷、漏洞等安全问题及其相应修改的文件及其路径、修改内容、存在漏洞文件版本号、修复漏洞补丁文件版本号、记录的日志信息；

2) 参照漏洞补丁提供者提供的说明材料，部署修补前后的被测设备，搭建测试环境。记录测试环境信息，信息内容参见附录表B.2；

3) 对漏洞补丁包/升级包进行一致性验证。记录验证信息，信息内容参见附录表B.3。

d) 预期结果：

1) 说明材料中明确包含补丁包/升级包的修改说明；

2) 漏洞补丁实际修补内容与漏洞修补说明一致。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.6 漏洞补丁动态验证

根据对相关漏洞的分析结果，对已公布POC的漏洞可进行动态验证，确认漏洞补丁对POC的有效性，即相关POC对修补后的被测设备不再有效。

该评估项包括如下内容：

a) 安全要求：

被测设备安装漏洞补丁后，通过POC代码应无法触发相关漏洞。

b) 预置条件：

漏洞补丁提供者提供说明材料或自验证证明材料，说明材料中包含漏洞补丁包/升级包的修改

说明，包括修补的安全缺陷、漏洞等安全问题及其相应修改的文件及其路径、修改内容、存在漏洞文件版本号、修复漏洞补丁文件版本号、记录的日志信息。记录漏洞补丁相关漏洞信息，信息内容参考附录表 B.4。

c） 检测方法：

1） 参照漏洞补丁提供者提供的说明材料，确认是否包含漏洞补丁包/升级包的修改说明，包括修补的安全缺陷、漏洞等安全问题及其相应修改的文件及其路径、修改内容、存在漏洞文件版本号、修复漏洞补丁文件版本号、记录的日志信息。

2） 参照网络产品和服务提供者提供的说明材料，部署修补前后的被测设备，搭建测试环境。记录测试环境信息，信息内容参考附录表 B.5。

3） 使用 POC 动态分析验证的方法对漏洞补丁包/升级包的有效性进行验证。通过 POC 代码对修补前后的目标环境进行漏洞发现，试图触发相关漏洞，并通过对照修补前后的调试信息或者状态结果来确定漏洞修补的有效性。记录验证信息，信息内容参考附录表 B.6。

d） 预期结果：

通过 POC 代码无法触发修补后被测设备的相关漏洞。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

附 录 A
（资料性）
漏洞补丁一致性分析方法

静态分析技术是对被分析目标的源程序进行分析检测，发现程序中存在的安全漏洞或隐患，是一种典型的白盒分析技术。它的方法主要包括静态字符串搜索、上下文搜索。

漏洞补丁一致性验证静态分析技术，是分析人员借助静态分析工具，对打补丁前后的文件进行内容检查、源代码分析或二进制文件分析，通过流程对比，发现字符串变化、边界值变化、函数参数变化等存在漏洞的位置和修补位置，进一步了解漏洞的细节，确认漏洞补丁实际修补内容与漏洞修补说明的一致性。

常用的补丁比对工具有 Beyond Compare、IDACompare、Binary Diffing Suite（EBDS）、BinDiff、NIPC Binary Differ（NBD）。此外大量的高级文字编辑工具也有相似的功能，如 Ultra Edit、HexEdit 等。

附 录 B
（资料性）
漏洞补丁信息记录表

B.1 漏洞补丁一致性验证漏洞信息记录表

漏洞补丁一致性验证漏洞信息记录内容见表B.1。

表B.1 漏洞补丁一致性验证漏洞信息记录表

补丁文件名称	补丁文件路径	存在漏洞文件版本号	修复补丁文件版本号	修复漏洞信息	修改内容	补丁日志信息
必填	必填	必填	必填	必填	选填	选填

B.2 漏洞补丁一致性验证环境信息记录表

漏洞补丁一致性验证环境信息记录内容见表B.2。

表B.2 漏洞补丁一致性验证测试环境信息记录表

靶机名称	快照名称	IP 地址	MAC 地址	漏洞相关信息	其他
必填	选填	必填	必填	必填	选填

B.3 漏洞补丁一致性验证信息记录表

漏洞补丁一致性验证信息记录内容见表 B.3。

表B.3 漏洞补丁一致性验证信息记录表

漏洞编号	验证结果	验证方式	靶机环境	文件信息	验证描述	其他
必填	必填	必填	必填	选填	必填	选填

B.4 POC动态分析验证信息记录表

POC动态分析验证信息记录内容见表B.4。

表B.4 POC动态分析验证信息记录表

补丁文件名称	补丁文件路径	存在漏洞文件版本号	修复补丁文件版本号	修复漏洞信息	修改内容	补丁日志信息
必填	必填	必填	必填	必填	必填	选填

B.5 POC动态分析验证测试环境信息记录表

POC动态分析验证测试环境信息记录内容见表B.5。

表B.5　POC动态分析验证测试环境信息记录表

靶机名称	快照名称	IP 地址	MAC 地址	漏洞相关信息	其他
必填	必填	必填	必填	必填	选填

B.6　POC动态分析验证信息记录表

POC动态分析验证信息记录内容见表B.6。

表B.6　POC动态分析验证信息记录表

漏洞编号	验证结果	验证方式	靶机环境	POC 信息	验证描述	其他
必填	必填	必填	必填	选填	必填	选填

参 考 文 献

[1] GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南
[2] GB/T 30276—2020 信息安全技术 网络安全漏洞管理规范

电信终端产业协会团体标准

漏洞补丁验证通用方法

T/TAF 166—2023

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn