修复安全终端上显示的漏洞

目录

简介

本文档介绍如何检查终端的思科风险评分并应用修复。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全终端控制台

使用的组件

本文档中的信息基于以下软件版本：

- 安全终端控制台v5.4.2025030619

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

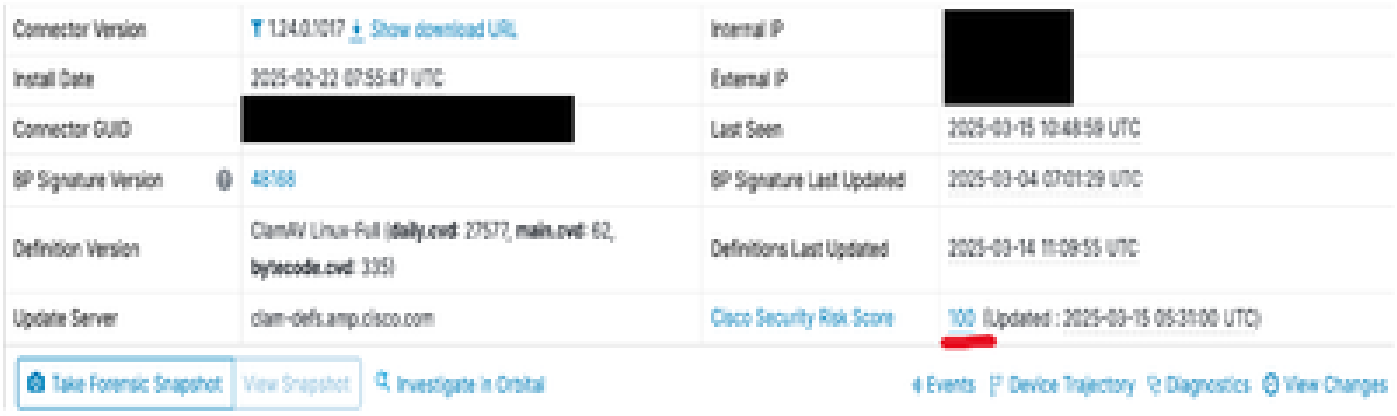
思科安全风险评分的等级范围为0到100。它通过技术严重性和现实世界的攻击者如何利用漏洞来量化漏洞风险。

检查终端的思科安全风险评分并应用建议的修复程序。

解决方案

1 — 要查看Cisco安全风险得分，请导航到Management > Computers并选择Cisco Security Risk Score显示：

2 — 您会看到计算机列表。展开要检查的计算机信息，然后点击显示的思科安全风险分数(Cisco Security Risk Score number)，如下所示：



3 — 您会看到影响终端的CVE列表。单击Fix Available，如下所示：

4 — 此处您可以看到下面列出的CVE的建议修复：

Vulnerability Fixes

CVE-2023-4863

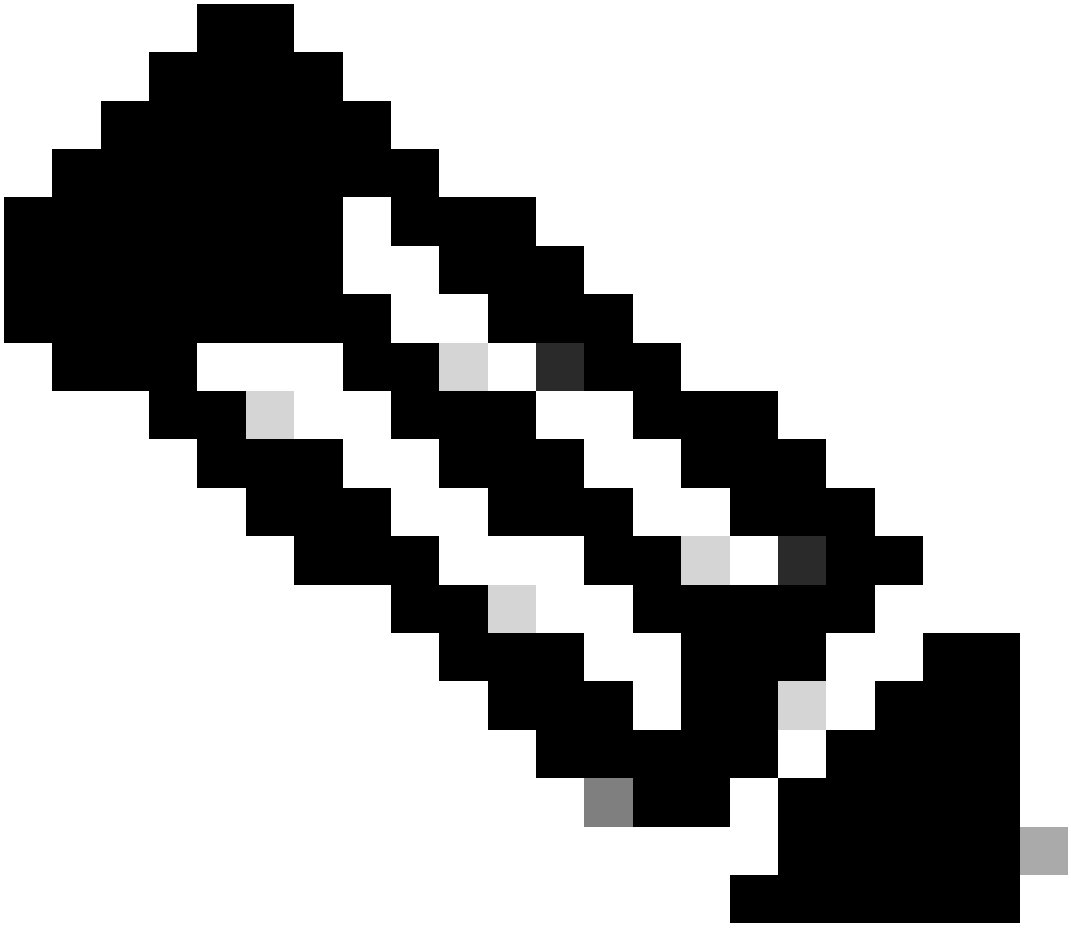
100 / 100
CVSS 3.1: 8.8

Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)

Fixed By:

- USN-6368-1

Close



注意：如果没有可用的修复，请联系TAC。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。