功能概述

在系统日常使用过程中有可能会出现系统漏洞，会导致系统出现稳定性或者兼容性异常；特别是安全漏洞，容易导致系统容易受到病毒估计，影响系统安全性。可以通过系统自带的更新功能进行系统漏洞修；也可以通过统信安全应急响应中心进行手动更新。

系统更新修复漏洞

在更新设置页面开启可从仓库更新类型中的“**系统**”、或“**仅安全更新**”后，自动检查、自动下载、自动安装、更新提醒才能正常操作。

系统：包括安全漏洞更新、系统环境更新、已安装应用更新等。

仅安全更新：只更新安全漏洞和兼容性相关的更新



系统更新设置

自定义修复漏洞

在检测出多个安全漏洞时，由于一些客观原因（内网环境，针对某个定制漏洞，第三方安全漏洞）无法通过 “**控制中心--更新--仅安全更新**” 进行修复，可以自行进行修复

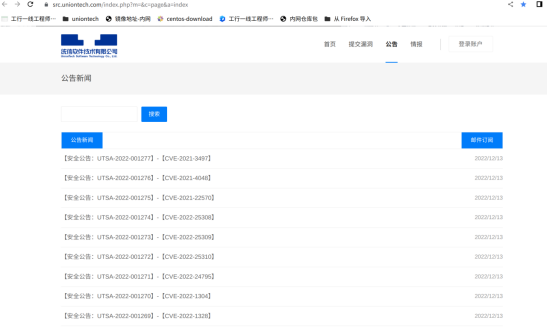
例如：安全漏洞(CVE-2021-3497)安全修复

* 统信安全应急响应中心修复

进入[统信安全应急响应中心](https://src.uniontech.com/)---**进入公告页面，漏洞安全页**



统信安全应急响应中心



漏洞安全页

根据【统信安全公告: UTSA-2022-001277】-【CVE-2021-3497】漏洞资料中的安全文档--“六：修复办法”进行漏洞修复。并根据“七：是否受影响判断”判断漏洞修复情况



统信安全公告

【注1】：统信操作系统专业版系统漏洞一直持续修复更新，建议在使用系统时， 更新至最新版本进行使用

【注2】：其他安全漏洞修复站点

<https://access.redhat.com/security/cve/CVE-2021-3497>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3497>

<https://nvd.nist.gov/vuln/detail/CVE-2021-3497>

 ©统信软件技术有限公司。访问者可将本网站提供的内容或服务用于个人学习、研究或欣赏，以及其他非商业性或非盈利性用途，但同时应遵守著作权法及其他相关法律的规定，不得侵犯本网站及相关权利人的合法权利。除此以外，将本网站任何内容或服务进行转载，须备注：**该文档出自【faq.uniontech.com】统信软件知识分享平台**。否则统信软件将追究相关版权责任。