

Fortinet 发布多款产品的安全加固版本 包含前沿 AI 修复及后续发布流程优化

Fortinet 已于今日（北京时间 2026 年 10 月 23 日）正式发布 FortiOS、FortiManager 和 FortiAnalyzer 的联合安全更新包。此次更新是继 FortiMail 和 FortiAuthenticator 新版发布后的持续推进。我们强烈建议每一位用户立即安排升级操作，并优先处理所有面向互联网的设备，以最大程度降低潜在安全风险。

本次发布的安全更新，包含针对我们前沿 AI 辅助安全测试项目（**Frontier AI-assisted security testing program**）所识别漏洞的修复措施。

这次版本升级有何不同？

Fortinet 已将前沿 AI 模型深度集成至产品安全测试流程中。这些模型能够以完全超越传统模糊测试和人工审计的深度与速度，全面分析代码路径、协议处理逻辑及配置逻辑。

这项工作能帮助我们更高效地发现潜在漏洞，以在恶意行为者发现并利用漏洞前，主动完成修复工作。这正是我们原生安全性承诺的落地实践：在源头识别并封堵漏洞。

同时，我们也对一项深层影响保持坦诚：同类 AI 能力正逐步为攻击者所掌握，尤其是随着开放权重模型的持续进步，这一趋势愈发明显。从漏洞披露到被利用之间的时间窗口正不断压缩，且我们预计这一趋势将持续收窄。

为何需立即升级？

我们强烈建议用户将本次升级视为高优先级事项而非例行维护，升级的紧迫性主要源于以下四个方面：

- 修复等级评估：**本批次版本覆盖了关键级（Critical）及高危级（High）的安全修复。
- 武器化速度显著提升：**借助 AI 工具，攻击者可在数小时到数天内逆向分析补丁并构建可利用的漏洞代码，无需耗费数周。
- 补丁比对风险：**补丁公开后，修复痕迹反而暴露了漏洞所在，未修复的设备将成为攻击者眼中更容易得手的目标。

4. **漏洞链利用**：攻击者能够利用 AI 技术将彼此孤立、低危的漏洞进行串联，组合成一个更易于利用的高危漏洞。

我们建议立即采取临时缓解措施，包括通过带外设备管理限制暴露面，以及在可行情况下，将资源纳入 VPN 或 SASE 保护范围内，并在正式补丁完成优先级评估前部署虚拟补丁。

受影响产品及建议升级版本

受影响产品	受影响版本	建议升级版本	发布日期（北京时间）
FortiOS 8.0	8.0.0–8.0.1	8.0.2 或更高版本	10 月 23 日
FortiOS 7.6	7.6.0–7.6.7	7.6.8 或更高版本	10 月 23 日
FortiOS 7.4	7.4.0–7.4.12	7.4.13 或更高版本	10 月 23 日
FortiOS 7.2	7.2.0–7.2.13	7.2.14 或更高版本	10 月 23 日

受影响产品	受影响版本	建议升级版本	发布日期（北京时间）
FortiManager 8.0	8.0.0–8.0.1	8.0.2 或更高版本	10 月 23 日
FortiManager 7.6	7.6.0–7.6.7	7.6.8 或更高版本	10 月 23 日
FortiManager 7.4	7.4.0–7.4.11	7.4.12 或更高版本	10 月 23 日
FortiManager 7.2	7.2.0–7.2.12	7.2.13 或更高版本	10 月 23 日

受影响产品	受影响版本	建议升级版本	发布日期（北京时间）
FortiAnalyzer 8.0	8.0.0–8.0.1	8.0.2 或更高版本	10 月 23 日

FortiAnalyzer 7.6	7.6.0–7.6.7	7.6.8 或更高版本	10 月 23 日
FortiAnalyzer 7.4	7.4.0–7.4.11	7.4.12 或更高版本	10 月 23 日
FortiAnalyzer 7.2	7.2.0–7.2.12	7.2.13 或更高版本	10 月 23 日

受影响产品	受影响版本	建议升级版本	发布日期（北京时间）
FortiMail 8.0	8.0.0–8.0.1	8.0.2 或更高版本	10 月 22 日
FortiMail 7.6	7.6.0–7.6.6	7.6.7 或更高版本	10 月 22 日
FortiMail 7.4	7.4.0–7.4.8	7.4.9 或更高版本	10 月 22 日
FortiMail 7.2	7.2.0–7.2.9	7.4 或更高版本	10 月 22 日

受影响产品	受影响版本	建议升级版本	发布日期（北京时间）
FortiAuthenticator 8.0	8.0.0–8.0.3	8.0.4 或更高版本	10 月 22 日
FortiAuthenticator 6.6	6.6.0–6.6.10	6.6.11 或更高版本	10 月 22 日

请注意，官方公告将于 11 月 10 日星期二（下一补丁发布日）正式对外发布。此举体现了 Fortinet 在兼顾客户安全与负责任的透明度之间所秉持的持续承诺。届时，这些公告将发布在 [Fortinet 产品安全事件响应团队（PSIRT）官方页面](#)。

- FortiSASE 已于 10 月 23 日（北京时间）发布前完成自动更新。

- FortiManager Cloud 版本已于 10 月 23 日（北京时间）前开放更新，但可能需手动更新。
- 公有云实例相关更新正由各云服务合作伙伴逐步推送中，请遵循各云平台的标准发布流程进行确认与操作。

即日起，应采取哪些行动？

新版本已于今日（北京时间 10 月 23 日）发布，请立即完成升级操作。

- **资产盘点：**全面清查并登记所有 FortiManager 设备及 FortiOS 实例，建立资产清单，并优先排查所有面向互联网暴露的资产。
- **安排维护窗口：**为面向互联网的系统优先预留 10 月 23 日至 24 日的升级操作窗口
- **备份配置：**在升级操作启动前，妥善保存当前设备的配置
- **持续监控：**在补丁部署前后，密切审查系统日志，重点关注异常的管理员权限访问行为及未经授权的配置篡改。

如您无法立即升级，可通过以下方式在此期间降低暴露风险：

- **限制管理接口暴露范围：**将管理接口（HTTPS、SSH）的访问权限严格限定于受信任的 IP 地址，或在面向外部网络的接口上直接将其禁用。
- **隔离管理通道：**确保 FortiManager 管理接口禁止公网暴露，阻断外部访问路径。

- 遵循以下最佳实践，包括：
 - 使用强密码并杜绝凭证复用
 - 对所有管理员账户强制执行多因素认证（MFA）

这些措施虽可降低风险，但不能取代及时升级的必要性。

Fortinet 的承诺

Fortinet 始终坚信，唯有厂商主动发现漏洞、及时修复，并以负责任的方式进行披露，广大客户方能获得更充分的保护。为持续领先同样运用前沿 AI 工具实施攻击的威胁行为者，我们已将前沿 AI 技术深度融入我们的漏洞检测流程。未来，我们将持续将这一方法推广至 Fortinet 全线产品，并本着安全透明的原则，将相关研究成果与广大客户充分共享。

感谢您对此安全事件的快速响应与积极配合。如需升级部署方面的技术支持，请随时联系 Fortinet 技术支持团队或您的专属客户经理。同时，建议您订阅 [FortiGuard PSIRT 安全公告](#)，以便在新版本正式发布当日第一时间获取更新详情与部署指引。