U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Privacy, Access, Civil Liberties, and Transparency
Washington, DC 20528

2024 年 6 月 20 日

尊敬的同事,

如**您所知**，**网**络安全和基础设施安全局（CISA）的化学品安全评估工具（CSAT）在 2024 年 1 月 23 日至 2024 年 1 月 26 日期间成为恶意行为者网络安全入侵的目标，导致可能未经授权访问人员担保计划提交的文件和化学恐怖主义脆弱性信息（CVI）授权用户的账户。

虽然 CISA 的调查没有发现这些数据被外泄的证据，但出于谨慎起见，我们还是通知了所有将个人身份信息 (PII) 提交给 CISA 的化学设施反恐标准 (CFATS) 计划进行审查或拥有 CVI 授权用户账户的个人，这些信息可能已被不当访问。我和你一样感到担忧和沮丧，并向你提供我们所知道的有关这次企图入侵的信息。

您收到此通知是因为（1）您曾进入限制区域和/或关键资产的化工设施，该设施可能已经向人员保障计划提交了您的个人可识别信息进行审查，或者（2）您或化工设施在2007年6月至2023年7月期间提交了有限的个人可识别信息和商务联系信息，以便创建CVI授权用户账户。我们还联系了您所在的化工厂，了解有关入侵的技术细节。

可能受到影响的信息

人员担保计划. CFATS 人员担保计划使受 CFATS 监管的设施能够遵守基于风险的绩效标准 (RBPS) 12(iv)--人员担保。RBPS 第 12(iv)条[1]要求对已经或正在设法进入高风险化学设施禁区和重要资产的设施人员和无陪同访客进行筛查，以确定他们是否与恐怖分子有潜在联系。这包括通过 CSAT 提交 PII 以进行直接审查，或重新利用国土安全部其他计划下进行的审查，以便根据恐怖分子筛查数据库对个人进行审查[2]。

通过人事担保计划提交的个人信息包括个人姓名、出生日期、公民身份或性别。如果有或需要，还提供了非美国人的其他个人信息，包括：

- 别名
- 出生地
- 国籍
- 护照号码
- 申诉编号
- A 编号

[1] 6 C.F.R. 27.230(a)12(iv)。
[2]有关恐怖分子筛查数据库的更多信息，请访问：https://www.fbi.gov/investigate/terrorism/tsc

- 全球入境 ID 编号
- TWIC ID 编号

CSAT 用户帐号。一般来说，为设施提交CSAT信息的用户账户有两种类型：提交或参与开发顶层调查、安全漏洞评估和场地安全计划（包括CVI授权用户）的CSAT用户，以及提交人员保障信息的CSAT用户。在这两种情况下，为创建 CSAT 账户而收集的信息都是一样的：姓名、职务、公司地址和公司电话号码。

入侵详情

1 月 26 日，CISA 发现了影响 CSAT Ivanti Connect Secure 设备的潜在恶意活动[3]。CISA 立即将系统下线，将应用程序与网络的其他部分隔离，并开始进行取证调查。此次调查包括来自 CISA 首席信息官办公室、网络安全部威胁猎杀小组和国土安全部网络运行中心的技术专家。

在调查过程中，我们发现恶意行为者在 Ivanti 设备上安装了高级 webshell。这类 webshell 可用于执行恶意命令或向底层系统写入文件。我们的分析进一步发现，一名恶意行为者在两天内多次访问了该 webshell。

重要的是，调查已经结束，并未发现 CSAT 数据泄露或 Ivanti 设备之外的对手访问。CSAT 中的所有信息都使用 AES 256 加密技术进行加密，每个应用程序的信息都有额外的安全控制措施，以限制横向访问的可能性。加密密钥被隐藏，以防止威胁行为者对系统的访问。

为受影响的个人提出的建议

虽然 调查没有发现凭证被盗的证据，但我们建议您阅读并遵循 CISA **关于如何保**护自己免受网络行为者暴力攻击的指南 (https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors), 选择密码并保护密码 (https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords), 和多重身**份**验证 (https://www.cisa.gov/MFA).

CISA 创建了一个网站，提供本通知的副本、常见问题、定期更新以及注册电子邮件发送列表以接收网站更新的机会。在 CISA 探索其他可能的补救措施的过程中，我们鼓励您注册加入我们针对此事件的发布列表，以便接收 www.cisa.gov/csat-notification 上的所有最新更新。受影**响的个人如**对此事件有任何疑问，请发送电子邮件至 CFATS.Notificiations@cisa.dhs.gov 联系 CISA 化学安全分部。

此致,

[3] 有关此类恶意活动的更多信息，请访问：https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

詹姆斯-伯德
首席隐私官