# CVE-2020-2021 | PAN-OS SAML 身份验证绕过漏洞通告

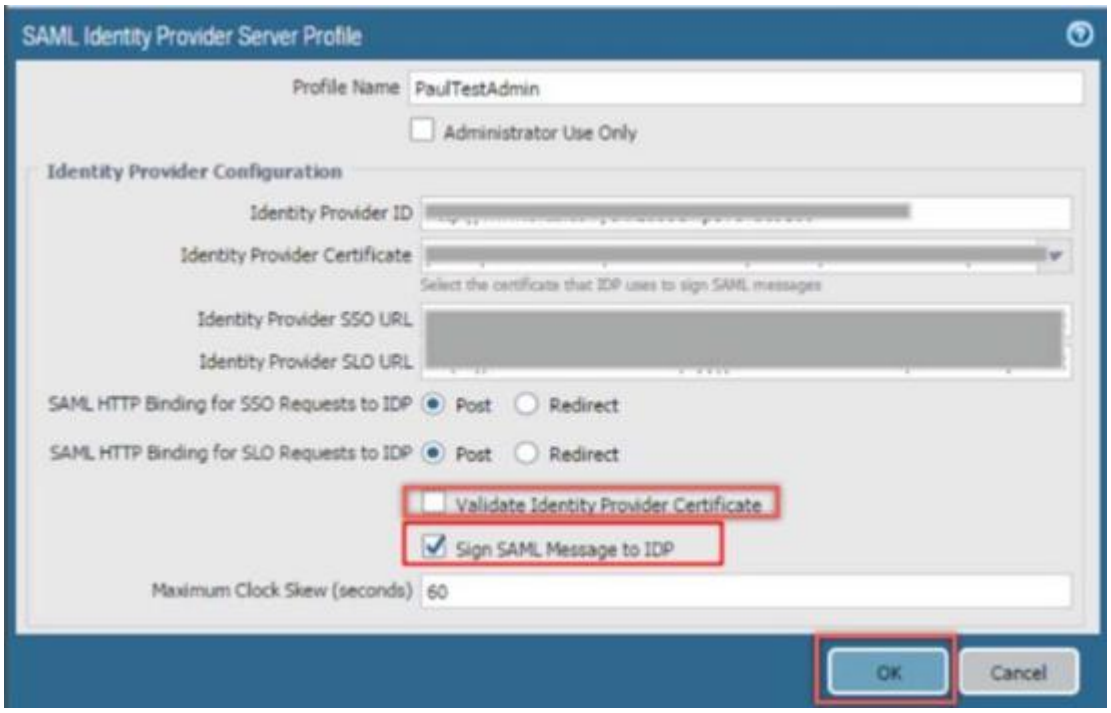
## 0x00 漏洞概述

| CVE ID | CVE-2020-2021 | 时 间 | 2020-06-30 |
|---|---|---|---|
| 类 型 | AB | 等 级 | 严重 |
| 远程利用 | 是 | 影响范围 | |

## 0x01 漏洞详情


2020 年 6 月 29 日，Palo Alto Networks 官方发布安全公告，修复了一个 PAN-OS SAML 身份验证绕过漏洞（CVE-2020-2021）。攻击者无需经过身份验证即可利用该漏洞访问设备。

在启用安全性断言标记语言（SAML）身份验证并禁用“验证身份提供商证书”选项时，由于 PAN-OS SAML 身份验证过程中没有正确地验证签名，导致未经身份验证的攻击者可以更改 PAN OS 的设置和功能。前提条件是攻击者必须可以访问易受攻击的服务器，才能利用此漏洞。




该漏洞是在 CVSSv3 严重等级中获得 10 分的罕见漏洞之一，既不需要高级技术技能，又可以通过 Internet 进行远程利用。美国网络司令部要求所有受 CVE-2020-2021 影响的设备立即修复该漏洞，并表示外国的 APT 组织可能很快就会尝试利用该漏洞发起攻击。

可以通过基于 SAML 的单点登录（SSO）身份验证保护的资源有：

GlobalProtect Gateway,

GlobalProtect Portal,

GlobalProtect Clientless VPN,

Authentication and Captive Portal,

PAN-OS next-generation firewalls (PA-Series, VM-Series) and Panorama web interfaces

Prisma Access

对于GlobalProtect 网关、GlobalProtect 门户、无客户端VPN、Captive Portal 和Prisma Access，未经身份验证的攻击者可以通过网络访问服务器上受保护的资源，不会影响网关，门户或 VPN 服务器的完整性和可用性，但攻击者无法检查或篡改普通用户的会话。这是一个严重级别的漏洞，CVSS 评分 10.0。

对于 PAN-OS 和 Panorama Web 界面，如果未经身份验证的攻击者具有对 PAN-OS 或 Panorama Web 界面的访问权，即可以管理员身份登录并执行管理操作。这是一个严重级别

的漏洞，CVSS 评分 10.0，如果仅可通过受限管理网络访问 Web 界面，则CVSS 评分 9.6。

以下是 CVE-2020-2021 漏洞影响的 Palo Alto Networks PAN-OS 版本：

| 版本号 | 受影响的 | 不受影响 |
| --- | --- | --- |
| 9.1 | <9.1.3 | > = 9.1.3 |
| 9.0 | <9.0.9 | > = 9.0.9 |
| 8.1 | <8.1.15 | > = 8.1.15 |
| 8.0 | 8.0。* | |
| 7.1 | | 7.1。* |

请相关用户尽快查看配置，及时确认是否受到该漏洞影响，具体方法如下：

- 仅当启用了 SAML 身份验证并且在“SAML 身份提供商服务器配置文件”中禁用“身份提供商证书”选项时，才可以利用该漏洞。
- 如果不使用 SAML 进行身份验证，则无法利用该漏洞。
- 如果在 SAML 身份提供商服务器配置文件中启用了“验证身份提供商证书”选项，则无法利用该漏洞。

关于如何检查服务器配置并实施缓解措施的说明，请参考：https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UXK

- 要检查是否在防火墙上启用了 SAML 身份验证，请参考 Device > Server Profiles > SAML Identity Provider；
- 要检查是否为Panorama 管理员身份验证启用了SAML 身份验证，请参考 Panorama > Server Profiles > SAML Identity Provider；
- 要检查是否为 Panorama 管理的防火墙启用了 SAML 身份验证，请参考 Device > [template]> Server Profiles > SAML Identity Provider。

根据配置，任何未经授权的访问都会记录在系统日志中，但是很难区分有效登录名和恶意登录名。

## 0x02 处置建议

官方已发布 PAN-OS 8.1.15、PAN-OS 9.0.9、PAN-OS 9.1.3 和更高版本，请相关用户及时升级。

**注意**：在升级到固定版本之前，请确保将 SAML 身份提供商的签名证书配置为“身份提供商证书”，以确保用户可以继续进行身份验证。请参考：https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-saml-authentication

- PAN-OS 升级之前和之后所需的所有操作的详细信息，请参考：https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UXK
- 为了清除 GlobalProtect 门户和网关上的未授权会话，Prisma Access 通过 Panorama 管理，请使用 Panorama 更改 Authentication Override cookie 的配置。请参考：https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UXy

重新启动防火墙和 Panorama 可以清除 Web 界面上的任何未经授权的会话。

- 要清除 Captive Portal 中的任何未授权用户会话，请执行以下步骤：

  运行以下命令

  ```
  show user ip-user-mapping all type SSO
  ```

  对于返回的所有 IP，请运行以下两个命令以清除用户：

  ```
  clear user-cache-mp <above ips>
  ```

  ```
  clear user-cache <above ips>
  ```

  - PAN-OS 8.0 已终止支持（截至 2019 年 10 月 31 日），不再维护。

所有 Prisma Access 服务均已升级以解决此问题，并且不再易受攻击。Prisma Access 客户不需要对 SAML 或 IdP 配置进行任何更改。

临时措施：

- 使用其他身份验证方法并禁用 SAML 身份验证；
- 在执行升级之前，同时应用（a）和（b）两项缓解措施。

（a） 确保已配置“身份提供商证书”。配置“身份提供商证书”是安全 SAML 身份验证配置的重要组成部分。

（b） 如果身份提供商（IDP）证书是证书颁发机构（CA）签名的证书，则确保在 SAML

身份提供商服务器配置文件中启用了“身份提供商证书”选项。默认情况下，许多流行的 IDP 都会生成自签名 IDP 证书，并且无法启用“验证身份提供商证书”选项。要使用由 CA 签名的证书，可能需要执行其他步骤。该证书可以由内部企业 CA，PAN OS 上的 CA 或公共 CA 签名。可在 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UXP 上获取有关在 IDP 上配置 CA 颁发的证书的说明。

## 0x03 相关新闻

https://www.zdnet.com/article/us-cyber-command-says-foreign-hackers-will-most-likely-exploit-new-pan-os-security-bug/

## 0x04 参考链接

https://security.paloaltonetworks.com/CVE-2020-2021?from=timeline&isappinstalled=0

## 0x05 时间线

2020-06-29 Palo Alto Networks 发布安全公告
2020-06-30 VSRC 发布漏洞通告