MS14-068 漏洞分析

1 MS14-068 概述

MS14-068 漏洞是域内最严重的漏洞之一，补丁号为 KB3011780，其允许任意用户提升到域管权限。漏洞影响 `Windows Server 2003` 到 `Windows Server 2012 R2` 期间的 Windows 版本，参考 Microsoft 安全公告。

2 PAC 签名

在了解漏洞原理之前，先介绍 PAC 签名相关内容。以下是 TGT 票据中 PAC 的结构：

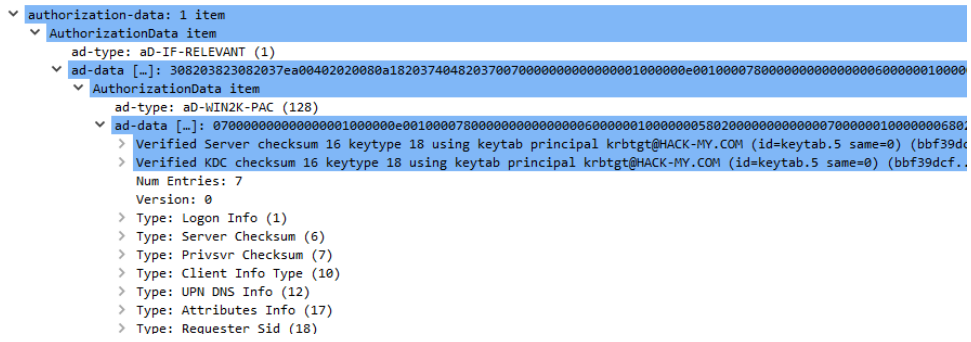

图 1: PAC 结构

其中 `Logon Info` 表明了客户端的身份信息，包括 SID、GroupID 等，结构参考 MS-PAC 规范。

`Server Checksum` 是服务校验和，`Privsvr Checksum` 是 KDC 校验和，分别由服务的 NTLM Hash 和 krbtgt 的 NTLM Hash 加密，用于防止 PAC 内容被篡改。

存在签名的原因有两个：

1. 带有服务 NTLM Hash 的签名，防止客户端生成自己的 PAC 并将其作为加密授权数据发送到 KDC，以包含在票据中。

2. 具有 KDC NTLM Hash 的签名，防止不受信任的服务伪造带有无效 PAC 的票据。

两个签名均为 PAC_SIGNATURE_DATA 结构：

```
typedef struct _PAC_SIGNATURE_DATA {
    ULONG SignatureType;
    UCHAR Signature[ANYSIZE_ARRAY];
} PAC_SIGNATURE_DATA, *PPAC_SIGNATURE_DATA;
```

SignatureType 类型如下：

Value	Meaning
KERB_CHECKSUM_HMAC_MD5 0xFFFFFF76	As specified in [RFC4120] and [RFC4757] section 4. Signature size is 16 bytes. Decimal value is -138.
HMAC_SHA1_96_AES128 0x0000000F	As specified in [RFC3962] section 7. Signature size is 12 bytes. Decimal value is 15.
HMAC_SHA1_96_AES256 0x00000010	As specified in [RFC3962] section 7. Signature size is 12 bytes. Decimal value is 16.

图 2: SignatureType 类型

Signature 即为校验和，长度由 SignatureType 决定。有时还可能存在 RODCIdentifier 字段，当 KDC 为 RODC 时，包含密钥版本号的前 16 位；当 KDC 不是 RODC 时，此字段不存在。

3 漏洞原理

该漏洞本质是 KDC 无法正确检查 Kerberos 票证请求随附的特权属性证书（PAC）中的有效签名，即服务校验和（Server Checksum）和 KDC 校验和（Privsvr Checksum）。签名规定使用 HMAC 系列的 checksum 算法，需要密钥（key）参与，但在实现中却允许所有 checksum 算法，包括 MD5。在不知道 krbtgt 的 NTLM Hash 和服务的 NTLM Hash（即不知道 key）的情况下，无法生成有效签名。若指定 MD5（无 key 的签名算法），可直接将 PAC 的校验和设为 MD5，并随意伪造 PAC 内容，生成 Server Checksum 和 Privsvr Checksum。

在 MS14-068 修补程序后，Microsoft 添加了验证步骤，确保校验和类型为 KRB_CHECKSUM_HMAC 阻止了无密钥算法。

需要修改 KERB_VALIDATION_INFO 结构中的字段，以伪造高权限 PAC：

其中 GroupIds 是用户所在组的 SID。只要将高权限组（如域管理员组）的 SID 添加到 GroupIds，服务在验证 TGS 时，域控会解密 PAC，提取 UserId 和 GroupIds。若伪造的 PAC 中 GroupIds 包含域管理员组信息，即可实现权限提升。

但伪造 TGT 需要知道 krbtgt 的 NTLM Hash。漏洞利用中，PAC 被加密后放入 enc-authorization-data，结构如下：

```
typedef struct _KERB_VALIDATION_INFO {
   FILETIME LogonTime;
   FILETIME LogoffTime;
   FILETIME KickOffTime;
   FILETIME PasswordLastSet;
   FILETIME PasswordCanChange;
   FILETIME PasswordMustChange;
   RPC_UNICODE_STRING EffectiveName;
   RPC_UNICODE_STRING FullName;
   RPC_UNICODE_STRING LogonScript;
   RPC_UNICODE_STRING ProfilePath;
   RPC_UNICODE_STRING HomeDirectory;
   RPC_UNICODE_STRING HomeDirectoryDrive;
   USHORT LogonCount;
   USHORT BadPasswordCount;
   ULONG UserId;
   ULONG PrimaryGroupId;
   ULONG GroupCount;
   [size_is(GroupCount)] PGROUP_MEMBERSHIP GroupIds;
   ULONG UserFlags;
   USER_SESSION_KEY UserSessionKey;
   RPC_UNICODE_STRING LogonServer;
   RPC_UNICODE_STRING LogonDomainName;
   PISID LogonDomainId;
   ULONG Reserved1[2];
   ULONG UserAccountControl;
   ULONG SubAuthStatus;
   FILETIME LastSuccessfulILogon;
   FILETIME LastFailedILogon;
   ULONG FailedILogonCount;
   ULONG Reserved3;
   ULONG SidCount;
   [size_is(SidCount)] PKERB_SID_AND_ATTRIBUTES ExtraSids;
   PISID ResourceGroupDomainSid;
   ULONG ResourceGroupCount;
   [size_is(ResourceGroupCount)] PGROUP_MEMBERSHIP ResourceGroupIds;
} KERB_VALIDATION_INFO, *PKERB_VALIDATION_INFO;
```

图 3: KERB_VALIDATION_INFO 结构

```
AuthorizationData ::= SEQUENCE OF SEQUENCE {
    ad-type[0] Int32,
    ad-data[1] OCTET STRING
}
```

ad-type 为加密算法，ad-data 为 PAC 加密后的内容，加密密钥由客户端生成。KDC 从 PA-DATA 中的 AP_REQ 获取该密钥，解密 ad-data 后得到 PAC 并验证校验和。正常 AP-REQ 阶段的 subkey 为 PAC 加密密钥：

将 PAC 放入 enc-authorization-data，KDC 能正确解析非 TGT 中的 PAC 信息，使用 subkey 解密并验证签名，返回带有伪造 PAC 的 TGS 票据，从而绕过签名验证，实现权限提升。

只需考虑 TGS-REQ 阶段的首次 PAC 签名验证，通过后返回的 TGS 票据可通过 AP-REQ 的 PAC 签名验证。

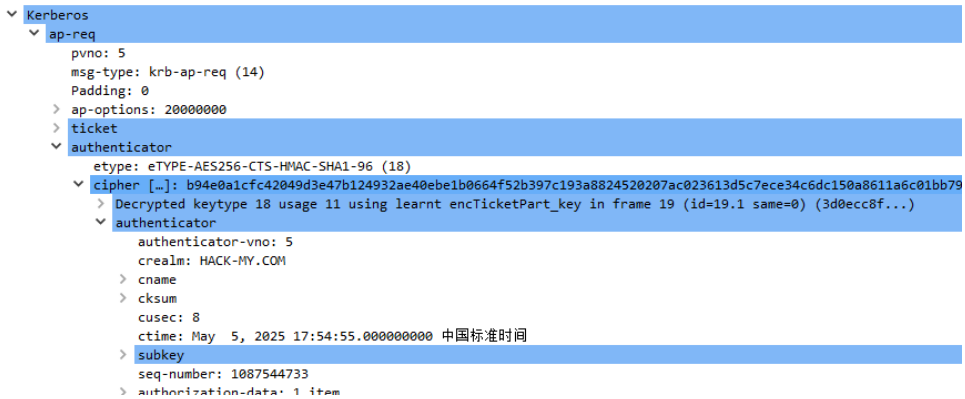

图 4: AP-REQ 阶段的 subkey

4 复现

Kerberos 的 AS-REQ 中有 include-pac 字段，决定 AS-REP 是否返回 PAC。攻击步骤如下：

1. 发起 AS-REQ 请求，include-pac 设为 false，返回的 TGT 不含 PAC。
2. 伪造 PAC，SID 为当前用户 SID，将以下组的 SID 添加到 GroupIds：
   - 域用户（513）
   - 域管理员（512）
   - 架构管理员（518）
   - 企业管理员（519）
   - 组策略创建者所有者（520）
3. 在 TGS-REQ 阶段，TGT 无 PAC，将伪造的 PAC 加密后放入 enc-authorization-data，加密密钥 subkey 放入 PA-DATA 的 AP_REQ，返回的 TGS 包含伪造的 PAC。
4. 执行 PTT 攻击。

4.1 MS14-068.exe

利用工具参考 GitHub 仓库。需获取 SID 作为 PAC Logon Info 结构的 UserId，保持原值即可：

执行命令：

```
MS14-068.exe -u HACK-WIN2008@hack-my.com -p 123qwe. -s S
   -1-5-21-4262386738-1606919640-785537236-1105 -d 192.168.30.10
```

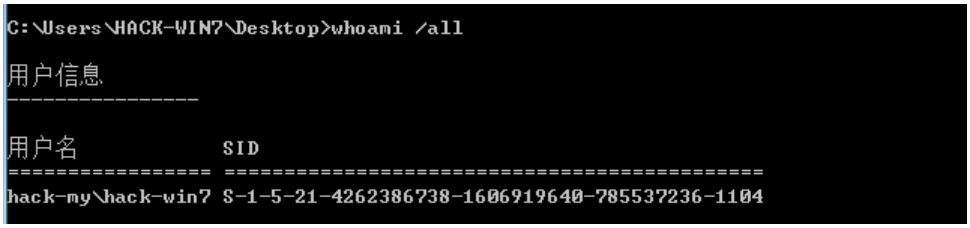

图 5: PAC Logon Info 结构

图 6: TGT 票据生成

生成 TGT 票据，使用 Mimikatz 注入，注入前清理现有票据，如图 7 所示。

在 Windows Server 2012 R2 未打 KB3011780 补丁的情况下，访问 DC 的 CIFS 服务显示不安全，表明已防御 MS14-068，如图 8 所示。

根据 文章，需将 DC 更换为 Windows Server 2008 或 Windows Server 2003 以复现，如图 9 和 10。

5 引用

Daiker, Windows Protocol: Kerberos, 2025.

Microsoft, MS-PAC: Logon Info, 2025.

Microsoft, MS-PAC: PAC_SIGNATURE_DATA, 2025.

Microsoft, Security Bulletin: MS14-068, 2014.

0range-x, MS14-068 原理浅析, 2021.

XZ Aliyun, MS14-068 相关文章, 2025.

Abatchy17, WindowsExploits: MS14-068, 2025.

图 7: Mimikatz 注入票据

图 8: CIFS 服务访问

官方通告，影响如下版本

Executive Summary

This security update resolves a privately reported vulnerability in Microsoft Windows Kerberos KDC that could allow an attacker to elevate unprivileged domain user account privileges to those of the domain administrator account. An attacker could use these elevated privileges to compromise any computer in the domain, including domain controllers. An attacker must have valid domain credentials to exploit this vulnerability. The affected component is available remotely to users who have standard user accounts with domain credentials; this is not the case for users with local account credentials only. When this security bulletin was issued, Microsoft was aware of limited, targeted attacks that attempt to exploit this vulnerability.

This security update is rated Critical for all supported editions of Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. The update is also being provided on a defense-in-depth basis for all supported editions of Windows Vista, Windows 7, Windows 8, and Windows 8.1. For more information, see the **Affected Software** section.

经复现，发现只有 Server 2003、2008 利用成功，继续翻看官方通告，发现指出对 Server 2012 实际上不受影响。

Kerberos Checksum Vulnerability - CVE-2014-6324

A remote elevation of privilege vulnerability exists in implementations of Kerberos KDC in Microsoft Windows. The vulnerability exists when the Microsoft Kerberos KDC implementations fail to properly validate signatures, which can allow for certain aspects of a Kerberos service ticket to be forged. Microsoft received information about this vulnerability through coordinated vulnerability disclosure. When this security bulletin was issued, Microsoft was aware of limited, targeted attacks that attempt to exploit this vulnerability. Note that the known attacks did not affect systems running Windows Server 2012 or Windows Server 2012 R2. The update addresses the vulnerability by correcting signature verification behavior in Windows implementations of Kerberos.

图 9: 文章建议

Kerberos 校验和漏洞 - CVE-2014-6324

Microsoft Windows 中 Kerberos KDC 的实现中存在远程特权提升漏洞。 当 Microsoft Kerberos KDC 实现无法正确验证签名时，存在此漏洞，这可以允许伪造 Kerberos 服务票证的某些方面。 Microsoft 通过协调的漏洞泄露收到了有关此漏洞的信息。 发布此安全公告时，Microsoft 知道尝试利用此漏洞的有限有针对性的攻击。 请注意，已知攻击不会影响运行 Windows Server 2012 或 Windows Server 2012 R2 的系统。 更新通过更正 Kerberos 的 Windows 实现中的签名验证行为来解决漏洞。

图 10: 环境要求