SOCNova

Tehdit ve Zafiyet İstihbarat Birimi

ZAFİYET ANALİZ RAPORU

CVE-2026-17106 | CopyEscape

Docker Container to Host Keyfi Dosya Yazma ve Yetki Yükseltme

Alan	Değer
Doküman Türü	Zafiyet Analiz ve Müdahale Rehberi
Doküman Sahibi	SOCNova | AI-Powered SOC Platform
Hazırlayan	SOCNova CTI Team
Yayın Tarihi	13 Ağustos 2026
Sürüm	v1.0
Gizlilik Sınıfı	**TLP:AMBER | Kuruma Özel**
Dağıtım	CISO, SOC Ekibi, Platform ve DevOps Mühendisliği, BT Operasyon

1. Yönetici Özeti

Imperva Red Team tarafından tespit edilen ve CVE-2026-17106 numarası ile takip edilen "CopyEscape" zafiyeti, Docker platformunun dosya kopyalama mekanizmasında yer alan bir hedef dışına yazma (destination escape) açığıdır. Zafiyet, kötü niyetli bir container içeriğini kopyalayan kullanıcının makinesinde, kullanıcının seçmiş olduğu hedef dizinin dışına dosya yazılmasına imkân tanımaktadır.

Bu zafiyetin kurumsal açıdan en kritik yanı, klasik bir container escape senaryosu olmamasıdır. Zafiyet container çalışma zamanında değil, Docker CLI tarafında tetiklenmektedir. Dolayısıyla sertleştirilmiş container runtime yapılandırmaları, seccomp profilleri veya AppArmor politikaları koruma sağlamamaktadır. Risk altındaki varlıklar CI/CD koşucu sunucuları, geliştirici iş istasyonları ve olay müdahale analistlerinin adli inceleme ortamlarıdır.

Zafiyetin sonucu, komutu çalıştıran kullanıcının yetkisi ile host üzerinde keyfi dosya yazma yeteneğidir. Linux tarafında kopyalama işleminin yükseltilmiş yetkilerle çalıştırılması durumunda, runc gibi sistem ikili dosyalarının üzerine yazılarak doğrudan root seviyesinde kod çalıştırma elde edilebilmektedir. macOS tarafında ise kabuk başlangıç betikleri, SSH yapılandırmaları ve LaunchAgent tanımlarının değiştirilmesi yolu ile kullanıcı seviyesinde kalıcılık sağlanabilmektedir.

Zafiyete ilişkin teknik analiz ve kavram ispatı detayları kamuya açıklanmış durumdadır. Bu nedenle silahlandırma süresinin kısa olacağı değerlendirilmekte, yamalamanın acil öncelik ile ele alınması tavsiye edilmektedir.

> **Yönetim Kararı:** Docker Engine ve CLI bileşenleri 29.7.2, Docker Desktop 4.86.0, Docker Sandboxes 0.38.0 sürümlerine yükseltilmelidir. Yamalama tamamlanana kadar yükseltilmiş yetki ile kopyalama kullanımı kurum genelinde yasaklanmalı ve kopyalama işlemleri yalnızca durdurulmuş container üzerinde yapılmalıdır.

2. Zafiyet Künyesi

Alan	Değer
CVE Kimliği	`CVE-2026-17106`
Kod Adı	CopyEscape
Danışmanlık Kaydı	`GHSA-hfg8-hc9c-6c3h`
Zafiyet Sınıfı	TOCTOU yarış koşulu ile birleştirilmiş sembolik bağlantı doğrulama hatası, hedef dışına arşiv çıkarma
CWE Eşleşmesi	CWE-367 (TOCTOU Race Condition), CWE-59 (Improper Link Resolution), CWE-22 (Path Traversal)
Etkilenen Bileşenler	`docker cp, sbx cp (Docker Sandboxes)`
Etkilenen Sürümler	Docker Engine ve CLI 29.7.2 öncesi, Docker Desktop 4.86.0 öncesi, Docker Sandboxes 0.38.0 öncesi
Keşfeden	Imperva Red Team

Alan	Değer
Açıklama Süreci	Nisan 2026 tarihinde başlatıldı, önceki düzeltmenin regresyonları nedeni ile birden fazla uzatma yapıldı
Kamuya Açıklanma	Ağustos 2026
PoC Durumu	**Kamuya açık teknik analiz ve PoC mevcut**
Aktif İstismar	Rapor tarihi itibarı ile doğrulanmış vahşi ortam istismarı bildirimi bulunmamaktadır

3. Teknik Analiz

3.1 Etkilenen Mekanizma

`docker cp` komutu, isminin aksine doğrudan bir dosya sistemi kopyalama işlemi gerçekleştirmemektedir. Kullanıcı `docker cp container:/path/file.txt ./file.txt` komutunu çalıştırdığında şu akış işletilir: Docker daemon container dosya sistemini gezerek talep edilen yolu bir tar arşivi içerisine paketler, oluşan arşiv Docker CLI tarafına teslim edilir ve CLI bu arşivi yerel makinede açar. Güvenlik sınırı bu noktada container değil, arşiv çıkarma işleminin kendisidir.

3.2 Kök Neden

Tasarım iki varsayıma dayanmaktadır. Birincisi daemon tarafından üretilen arşivin tutarlı olması, ikincisi CLI tarafından çıkarılan her dosyanın kullanıcı tarafından seçilen hedef dizin içerisinde kalmasıdır. Zafiyet, bu iki varsayımın tek bir kopyalama işlemi içerisinde birlikte kırılmasından kaynaklanmaktadır.

Docker, arşiv oluşturma sırasında yalnızca kendi iç durumunu kilitlemekte, container içerisinde çalışan süreçleri kilitlememektedir. Bu durum, saldırganın tarama devam ederken container dosya sistemini değiştirmesine olanak tanır. Zamanlanmış dizin değiştirme dizisi kullanan kötü niyetli container, Docker tarayıcısına önce bir dizin kaydettirmekte, ardından bu dizini sessizce hedef dizin dışına işaret eden bir sembolik bağlantı ile değiştirmektedir.

Çıkarma kodundaki doğrulama kontrolü inşa edilmiş bir yolu incelemekte, ancak sembolik bağlantı pratikte farklı ve doğrulanmamış bir arşiv yolu kullanılarak oluşturulmaktadır. Bu tutarsızlık, saldırgan kontrolündeki dosyaların sembolik bağlantının işaret ettiği konuma yazılmasını sağlamakta ve izolasyon sınırını tamamen devre dışı bırakmaktadır.

3.3 Saldırı Zinciri

Adım	Faaliyet	Açıklama
1	Teslimat	Kötü niyetli imaj veya ele geçirilmiş container kurban ortamına yerleştirilir. CI/CD tedarik zinciri, harici imaj kayıtları veya yapay zekâ kodlama ajanı sandbox çıktısı yaygın vektörlerdir.
2	Tetikleme	Kurban rutin bir kopyalama işlemi başlatır. Yapı artifaktlarının toplanması, log çıkarılması veya adli delil alınması tipik tetikleyicilerdir.
3	Yarış Koşulu	Container içerisindeki süreç, daemon tarama yaparken dizini sembolik bağlantı ile değiştirir.
4	Hedef Dışına Yazma	CLI arşivi açarken dosyaları sembolik bağlantının işaret ettiği konuma yazar. Örneğin /usr/bin dizini.
5	Kod Çalıştırma	Linux tarafında runc ikili dosyasının üzerine yazılması ile root seviyesinde, macOS tarafında kabuk yapılandırması veya LaunchAgent üzerinden kullanıcı seviyesinde kod çalıştırma elde edilir.

3.4 Platform Bazlı Etki

- **Linux:** Kopyalama işlemi yükseltilmiş yetkilerle çalıştırılıyorsa, yazma yeteneği `runc` gibi sistem ikili dosyalarını değiştirmek için kullanılabilir. Bu durumda komut tamamlandıktan hemen sonra root seviyesinde kod çalıştırma elde edilir. Otomasyon senaryolarında yükseltilmiş yetki kullanımı yaygın olduğu için bu senaryonun gerçekleşme olasılığı yüksektir.
- **macOS:** Docker Desktop daemon bileşeni bir sanal makine içerisinde çalışsa da CLI dosyaları yerelde çıkarmaya devam etmektedir. Saldırgan kabuk başlangıç betiklerini, SSH yapılandırmasını veya LaunchAgent tanımlarını değiştirerek kullanıcının bir sonraki terminal açılışında kod çalıştırabilir.
- **Yapay Zekâ Ajan Ortamları:** Docker Sandboxes bileşeni izole ajan ortamı ile host arasında dosya taşımak için `sbx cp` komutunu kullanmaktadır. Güvenilmeyen bir kodlama ajanı sandbox ortamından artifakt çekilmesi aynı sınıf hedef dışına çıkma riskini doğurmaktadır.

4. Risk Değerlendirmesi

4.1 Şiddet ve Risk Skoru

Metrik	Değerlendirme
Severity	**HIGH (Yüksek)**
SOCNova Risk Skoru	**8.4 / 10**
İstismar Karmaşıklığı	Yüksek. Başarılı istismar için yarış koşulunun kazanılması gerekmektedir. Ancak kamuya açık PoC bu engeli büyük ölçüde ortadan kaldırmaktadır.

Metrik	Değerlendirme
Gerekli Erişim	Kurbanın kötü niyetli container üzerinde kopyalama işlemi başlatması gerekmektedir. Doğrudan uzaktan istismar mümkün değildir.
Elde Edilen Yetki	Komutu çalıştıran kullanıcı yetkisi. Yükseltilmiş yetki veya root koşucu kullanımında root.
Maruziyet Yüzeyi	CI/CD koşucuları, geliştirici iş istasyonları, olay müdahale ortamları, yapay zekâ ajan sandbox ortamları
İş Etkisi	Yapı hattının ele geçirilmesi ile tedarik zinciri kompromizasyonu, kaynak kod ve kimlik bilgisi sızıntısı, kalıcı erişim

Resmî CVSS vektörü rapor tarihi itibarı ile kaynaklarda yayınlanmamıştır. Yukarıdaki risk skoru, SOCNova varlık kritikliği ve maruziyet modeline göre hesaplanmış kurum içi bir değerdir. Resmî CVSS yayınlandığında bu bölüm güncellenecektir.

4.2 Senaryo Bazlı Risk

Bu zafiyetin en dikkat çekici yanı, savunma faaliyetinin bizzat saldırı tetikleyicisi hâline gelmesidir. Ele geçirilmiş bir container üzerinden inceleme amacı ile delil çeken bir olay müdahale analisti, farkında olmadan istismarı tetikleyebilmektedir. Bu nedenle olay müdahale prosedürlerinin bu zafiyet dikkate alınarak revize edilmesi zorunludur.

5. MITRE ATT&CK Eşleştirmesi

Teknik ID	Teknik Adı	Bu Zafiyetteki Karşılığı
T1610	Deploy Container	Kötü niyetli imajın veya sandbox ortamının kurban ortamına yerleştirilmesi
T1611	Escape to Host	Kopyalama işlemi aracılığı ile container sınırı dışına dosya yazılması
T1068	Exploitation for Privilege Escalation	Yükseltilmiş yetkili kopyalama işleminde root seviyesine çıkılması
T1554	Compromise Host Software Binary	runc ve benzeri sistem ikili dosyalarının üzerine yazılması
T1546.004	Unix Shell Configuration Modification	bashrc, zshrc ve profile dosyalarının değiştirilerek kalıcılık sağlanması
T1543.001	Create or Modify System Process: Launch Agent	macOS LaunchAgent tanımlarının oluşturulması
T1098.004	SSH Authorized Keys	authorized_keys ve SSH yapılandırma dosyalarının değiştirilmesi
T1195.002	Supply Chain Compromise: Software Supply Chain	Güvenilmeyen imaj üzerinden CI/CD koşucusunun ele geçirilmesi

Teknik ID	Teknik Adı	Bu Zafiyetteki Karşılığı
T1036.005	Masquerading: Match Legitimate Name or Location	Meşru sistem yolunda sahte ikili dosya barındırılması

6. Tespit Yöntemleri

6.1 Varlık Envanteri ve Maruziyet Tespiti

En yüksek getiriyi sağlayan ilk adım, ortamdaki sürüm envanterinin çıkarılmasıdır. Aşağıdaki komut ile tespit edilen ve eşik değerlerin altında kalan tüm varlıklar zafiyetli kabul edilmelidir.

```
docker version --format 'Server: {{.Server.Version}} | Client: {{.Client.Version}}'
```

- Docker Engine ve CLI sürümü 29.7.2 altında ise zafiyetlidir
- Docker Desktop sürümü 4.86.0 altında ise zafiyetlidir
- Docker Sandboxes sürümü 0.38.0 altında ise zafiyetlidir

6.2 Süreç Telemetrisi

EDR ve auditd kaynaklarından `docker cp` ile `sbx cp` çalıştırmaları izlenmelidir. Özellikle üst sürecin sudo olduğu veya kullanıcının root olduğu çalıştırmalar, üretim ortamında neredeyse hiçbir zaman meşru değildir ve tek başına yüksek doğrulukta bir alarm üretir. CI/CD koşucu bağlamında güvenilmeyen veya harici imajlar ile korele edilmesi tavsiye edilir.

6.3 Dosya Bütünlüğü İzleme

Asıl tespit noktası burasıdır. Docker süreç ağacından kaynaklanan ve hedef dizin dışına yapılan dosya yazma işlemleri izlenmelidir. İzlenmesi gereken kritik yollar aşağıda listelenmiştir.

```
/usr/bin/runc          /usr/local/bin/*        /usr/bin/docker*
/etc/sudoers.d/*       /etc/cron.d/*           /etc/ld.so.preload
~/.bashrc              ~/.zshrc                ~/.profile
~/.ssh/config          ~/.ssh/authorized_keys
~/Library/LaunchAgents/*   (macOS)
```

Örnek auditd kural seti:

```
-w /usr/bin/runc -p wa -k socnova_copyescape_runc
-w /usr/local/bin -p wa -k socnova_copyescape_bin
-a always,exit -F arch=b64 -S symlinkat,renameat2 \
   -F dir=/var/lib/docker/overlay2 -k socnova_copyescape_race
```

6.4 Davranışsal Tespit

- Kısa bir zaman penceresi içerisinde aynı inode üzerinde yoğun rename ve symlink döngüsü gözlenmesi yarış koşulunun imzasıdır. Normal bir kopyalama işleminde saniyeler içerisinde onlarca dizin değiştirme işlemi beklenmez.
- Container overlay2 upperdir katmanında, mutlak host yollarına işaret eden sembolik bağlantı oluşturulması anormal kabul edilmelidir.
- Kopyalama işlemi sonrasında kullanıcının hedef dizini dışında oluşan yeni dosyaların varlığı incelenmelidir.
-

6.5 Korelasyon Mantığı

Süreç telemetrisi ve dosya bütünlüğü alarmları tek başlarına gürültü üretme eğilimindedir. SOCNova yaklaşımı, iki sinyalin altmış saniyelik bir pencere içerisinde korele edilmesidir. Bu korelasyon neredeyse tam isabet sağlamakta ve yanlış pozitif oranını kabul edilebilir seviyeye indirmektedir.

7. Detection Rule

Aşağıdaki Sigma kuralları SOCNova Tehdit ve Zafiyet İstihbarat Birimi tarafından hazırlanmış olup, kurumsal SIEM ve EDR platformlarına doğrudan yüklenebilir niteliktedir. Kuralların üretim ortamına alınmadan önce yedi günlük bir gözlem modunda çalıştırılması tavsiye edilir.

7.1 SOCNova-DET-2026-17106-01: Yetkili Kopyalama Komutu Çalıştırması

```
title: Docker CopyEscape - Privileged docker cp or sbx cp Execution
id: 6f2a91c4-8d13-4b7e-a5c0-1e93b7d2af58
status: experimental
description: |
  CVE-2026-17106 (CopyEscape) istismarinin birincil tetikleyicisini tespit eder.
  Yukseltilmis yetki ile calistirilan docker cp veya sbx cp komutlari, kotu
  niyetli bir container tarafindan host uzerinde keyfi dosya yazma ve root
  seviyesinde kod calistirma icin kullanilabilir.
author: SOCNova
date: 2026/08/13
modified: 2026/08/13
references:
    - https://www.imperva.com/blog/copyescape-taking-over-docker-hosts-with-docker-cp/
    - https://github.com/advisories/GHSA-hfg8-hc9c-6c3h
tags:
    - attack.privilege_escalation
    - attack.defense_evasion
    - attack.t1611
    - attack.t1068
    - attack.t1610
    - cve.2026.17106
logsource:
    category: process_creation
    product: linux
detection:
    selection_binary:
        Image|endswith:
            - '/docker'
            - '/sbx'
    selection_subcommand:
        CommandLine|contains:
            - ' cp '
            - ' container cp '
    selection_privileged:
        - ParentImage|endswith:
              - '/sudo'
              - '/doas'
        - User:
              - 'root'
        - CommandLine|startswith:
              - 'sudo '
    filter_approved_automation:
        ParentCommandLine|contains:
            - '/opt/socnova/approved-pipeline/'
    condition: selection_binary and selection_subcommand and
        selection_privileged and not filter_approved_automation
fields:
    - User
    - CommandLine
    - ParentImage
    - ParentCommandLine
    - CurrentDirectory
falsepositives:
    - Onaylanmis yedekleme ve artifakt toplama otomasyonlari
    - Adli inceleme sirasinda analistin bilincli kopyalama islemi
level: high
```

7.2 SOCNova-DET-2026-17106-02: İstismar Sonrası Kritik Dosya Üzerine Yazma

```
title: Docker CopyEscape - Host File Overwrite by Docker CLI
id: 3c81d47b-2a9f-4e60-b1d8-7f45c0e6ab92
status: experimental
description: |
  Docker CLI surec agacindan kaynaklanan ve sistem ikili dosyalari, kabuk
  yapilandirmalari, SSH ayarlari veya kalicilik konumlarina yapilan yazma
  islemlerini tespit eder. CVE-2026-17106 istismarinin ikinci asamasidir.
author: SOCNova
date: 2026/08/13
references:
    - https://www.imperva.com/blog/copyescape-taking-over-docker-hosts-with-docker-cp/
tags:
    - attack.persistence
    - attack.privilege_escalation
    - attack.t1554
    - attack.t1546.004
    - attack.t1543.001
    - attack.t1098.004
    - cve.2026.17106
logsource:
    category: file_event
    product: linux
detection:
    selection_process:
        Image|endswith:
            - '/docker'
            - '/dockerd'
            - '/sbx'
    selection_system_binary:
        TargetFilename|startswith:
            - '/usr/bin/'
            - '/usr/sbin/'
            - '/usr/local/bin/'
            - '/etc/sudoers.d/'
            - '/etc/cron.d/'
    selection_persistence_file:
        TargetFilename|endswith:
            - '/runc'
            - '/.bashrc'
            - '/.zshrc'
            - '/.profile'
            - '/.ssh/config'
            - '/.ssh/authorized_keys'
            - '/ld.so.preload'
    condition: selection_process and 1 of selection_system_binary,
        selection_persistence_file
fields:
    - TargetFilename
    - Image
    - User
    - ProcessId
falsepositives:
    - Docker paket yukseltme islemleri sirasinda olusan mesru yazmalar
level: critical
```

7.3 SOCNova-DET-2026-17106-03: Doğrulanmış İstismar Zinciri Korelasyonu

```
title: Docker CopyEscape - Confirmed Exploitation Chain
id: a94e7f30-15bc-42d8-9c6a-8b207e3f14d5
status: experimental
description: |
  Yetkili kopyalama komutunun ardindan altmis saniye icerisinde kritik dosya
  uzerine yazma gozlenmesi, CVE-2026-17106 istismarinin dogrulanmis
  gostergesidir. Tekil kurallarin gurultusunu ortadan kaldirir.
author: SOCNova
date: 2026/08/13
tags:
    - attack.privilege_escalation
    - attack.t1611
    - cve.2026.17106
correlation:
    type: temporal
    rules:
        - 6f2a91c4-8d13-4b7e-a5c0-1e93b7d2af58
        - 3c81d47b-2a9f-4e60-b1d8-7f45c0e6ab92
    group-by:
        - ComputerName
```

```
        - User
    timespan: 1m
falsepositives:
    - Bilinen bir yanlis pozitif senaryosu tespit edilmemistir
level: critical
```

Not: Sigma kural gövdeleri, farklı SIEM dönüştürücüleri ve YAML ayrıştırıcıları ile uyum sorunu yaşanmaması için ASCII karakter seti ile yazılmıştır. Bu bilinçli bir tercihtir.

8. Yamalama ve Kalıcı Çözüm

Kalıcı çözüm yamalamadır. Yazma işlemini gerçekleştiren bileşen daemon değil CLI olduğu için, yamanın öncelikli olarak istemci tarafında uygulanması kritik önemdedir. Sadece sunucu tarafının güncellenmesi koruma sağlamaz.

Bileşen	Güvenli Sürüm	Öncelik
Docker Engine ve CLI	`29.7.2 ve üzeri`	**P1 - Acil**
Docker Desktop	`4.86.0 ve üzeri`	**P1 - Acil**
Docker Sandboxes	`0.38.0 ve üzeri`	P2 - Yüksek

Açıklama süreci sırasında önceki bir düzeltmenin regresyonları nedeni ile birden fazla uzatma yapılmıştır. Bu nedenle ara sürümlere güvenilmemeli, doğrudan yukarıda belirtilen sürümlere çıkılmalıdır.

Debian ve Ubuntu

```
sudo apt-get update
sudo apt-get install --only-upgrade docker-ce docker-ce-cli containerd.io
docker version --format '{{.Client.Version}}'
```

RHEL, Rocky ve AlmaLinux

```
sudo dnf update docker-ce docker-ce-cli containerd.io
sudo systemctl restart docker
docker version --format '{{.Client.Version}}'
```

Docker Desktop

Geliştirici iş istasyonlarında sürüm 4.86.0 ve üzerine yükseltilmelidir. Kurumsal dağıtım araçları üzerinden zorunlu güncelleme politikası tanımlanması ve kullanıcı inisiyatifine bırakılmaması tavsiye edilir.

9. Telafi Edici Kontroller

Yamalama tamamlanana kadar aşağıdaki kontroller uygulanmalıdır. Kontroller etkinlik sırasına göre listelenmiştir.

1. Yükseltilmiş yetki ile kopyalama kullanımı kurum genelinde yasaklanmalıdır. Sudoers yapılandırmasında açık reddetme kuralı tanımlanmalı, CI/CD hatlarında statik tarama ile bu kullanım tespit edildiğinde yapı kırılmalıdır. Tek başına bu kontrol, root seviyesine giden yolu kapatmaktadır.
2. Canlı container üzerinden kopyalama yapılmamalıdır. Container önce durdurulmalı, kopyalama sonrasında tekrar başlatılmalıdır. Yarış koşulu container içerisinde çalışan bir süreç gerektirdiğinden, durdurulmuş container üzerinde istismar çalışmaz.
3. Güvenilmeyen container verisi yalnızca tek kullanımlık ve izole sanal makine ortamları üzerinden alınmalıdır. Olay müdahale prosedürleri bu yönde güncellenmelidir.
4. Alternatif olarak imaj dışarı aktarılarak, çıkarma işlemi ayrı ve kısıtlı bir dizinde gerçekleştirilebilir. Salt okunur bind mount kullanımı da uygun bir alternatiftir.
5. Docker grubu üyelikleri gözden geçirilmelidir. Bu grup zaten root eşdeğeri yetki taşımaktadır, CopyEscape yalnızca bu yetkinin istismar maliyetini düşürmüştür.
6. CI/CD koşucularının rootless çalışma moduna taşınması orta vadeli hedef olarak planlanmalıdır.

10. Aksiyon Planı

No	Aksiyon	Sorumlu	Hedef Süre
1	Docker sürüm envanterinin çıkarılması ve zafiyetli varlık listesinin oluşturulması	BT Operasyon	24 saat
2	Yükseltilmiş yetki ile kopyalama kullanımının yasaklanması ve hat kontrollerinin devreye alınması	DevOps Mühendisliği	24 saat
3	SOCNova Sigma kurallarının SIEM üzerine yüklenmesi ve gözlem moduna alınması	SOC Ekibi	48 saat
4	CI/CD koşucuları üzerinde yamalama çalışmasının tamamlanması	Platform Mühendisliği	72 saat
5	Olay müdahale ve adli inceleme prosedürlerinin revize edilmesi	SOC Ekibi	5 iş günü
6	Geliştirici iş istasyonlarında Docker Desktop yükseltmesinin tamamlanması	BT Operasyon	10 iş günü
7	Rootless koşucu geçiş planının hazırlanması	Platform Mühendisliği	30 gün

11. Değerlendirme

CopyEscape, container güvenliğine dair yerleşik bir varsayımı sorgulatmaktadır. Güvenlik sınırı yalnızca container çalışma zamanı değildir. Arşiv çıkarma işleminin kendisi de bir güvenlik sınırıdır ve sembolik bağlantılar ile eş zamanlı dosya değişiklikleri devreye girdiğinde, yol dizesi üzerinden yapılan kontroller bu sınırı garanti edememektedir.

Kurumsal açıdan çıkarılacak ders, yamalanması gereken varlığın sunucu filosu değil, geliştirici iş istasyonları ve yapı hattı koşucuları olduğudur. Önceliklendirme bu doğrultuda yapılmalıdır.

12. Referanslar

- Imperva Threat Research, CopyEscape: Taking Over Docker Hosts with docker cp
- GitHub Security Advisory, GHSA-hfg8-hc9c-6c3h
- Docker Engine ve CLI 29.7.2 sürüm notları
- Docker Sandboxes 0.38.0 sürüm notları, 6 Ağustos 2026
- NHS England Digital, Docker Releases Security Updates for Docker Copy Functionality
- MITRE ATT&CK Enterprise Matrix