

Ransomware

BOOM!

CVE-2023-21329

CVE-2023-21529

CVE-2020-9715

Emergency Incident

27 Apr 2026

ال Medusa
كتشف الداتا!



Privilege escalation

CLANG!

ديروا
update دابا!

2012 → 2023 → 2025 → 2026

BOD 22-01
— compliance

TICK!

شوف HTTP logs
هاد SQL injection واضح!

CVE-2023-21529

CVE-2020-9715

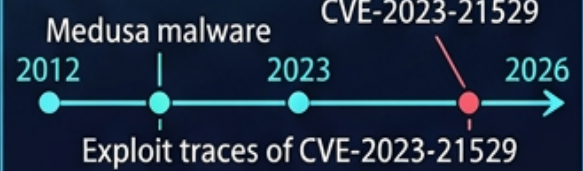
ZING!

Defused Cyber:
exploitation
بدا من 24 مارس

Unexpected
reappearance of
CVE-2012-1854
note.

TICK!

Timeline



ZING!

Storm-1175



HTTP req

<+1 payload
crafted
http=
stegner

Exploit traces

crafted data=...
<crafted dste='...'
<comen ->227
<payload can payloads ->...
<payloads

Medusa 2022-2153: 2
2022-2159: S
Medusa

ديرنا patches:
،Fortinet،
،Exchange،
!Adobe!



Fortinet: SUCCESS
Exchange: PATCHED
Adobe: UPDATED
Windows CLFS: SECURE
Host Process Fixes: APPLIED
VBA Mitigations: ASTI9E

Patch Complete
Integrity OK
KEV Updated

Deploy Patch

BOD 22-01
Compliance



SHING!

CVE Card
Vulnerable

CVE Card
Mitigated

Fortinet: SUCCESS
Patch Complete
Integrity OK
KEV Updated

KIRA
KIRA



27 أبريل قرب -
ربحنا المعركة!

