

Defending against Critical Vulnerabilities by Preventing Lateral Movement

Routing Scenario	LAN Protection	Internet Protection	Geo-Fencing Protection	Explanation
A	✗	✗	✓	These scenarios, which allow both LAN and Internet access, are vulnerable to this attack when no geo-blocking is in place. However, if the attacking IP originates from a blocked country, the exploit becomes impossible.
B	✗	✗	✓	
C	✗	✗	✓	
D	✓	✗	✓	Scenario D, which allows Internet access, is vulnerable to this attack when no geo-blocking is in place. However, if the attacking IP originates from a blocked country or the LAN, the exploit becomes impossible.
E	✓	✓	N/A	These Scenarios are immune to this exploit as they block both LAN and Internet access.
F	✓	✓	N/A	
G	✓	✓	N/A	
H	✓	✗	✓	Scenario H, which allows Internet access, is vulnerable to this attack when no geo-blocking is in place. However, if the attacking IP originates from a blocked country or the LAN, the exploit becomes impossible.

BYOS www.byos.io [in](#) [X](#) [@ByosTech](#)

The Oligo research team has uncovered a severe vulnerability dubbed "0.0.0.0 Day," on all major consumer Operating Systems. This vulnerability has been dormant for 18 years.


It exposes a fundamental weakness in browser network request handling, potentially granting malicious actors access to sensitive services on local devices.

Why is this significant?

While this specific vulnerability will eventually be patched, it highlights a crucial cybersecurity concern: the potential for rapid lateral movement across networks when application layer vulnerabilities are exploited.

Key takeaways:

- Any device on the local network could be at risk
- Application layer bugs are frequent, necessitating robust protective measures
- Lateral movement prevention is critical in modern cybersecurity strategies

Enter Byos: Your Defense Against Lateral Movement Attacks 

Byos delivers unmatched protection, regardless of asset vulnerability or attacker sophistication:

- 1 Decoupled Security: Byos operates independently from protected devices, ensuring robust defense against evolving threats.
- 2 Granular Control with Routing Scenario Policy + Secure Lobby SDN Overlay™ :
 - Scenarios E, F, G: Complete attack prevention through internet isolation
 - Scenarios A, B, C, D, H: Lateral movement blocked via country-based geo-fencing
- 3 Proactive Defense: Byos-protected devices remain immune to infections from compromised devices attempting lateral spread via LAN.

Don't let your network fall victim to the next "0.0.0.0 Day." Strengthen your defenses with Byos – where lateral movement meets its match.