

TECHNICAL ADVISORY

CVE-2026-70111: Windows Kernel Elevation of Privilege via DFS Referral Parsing

Corelight Research found a vulnerability in `mup.sys`, the Windows kernel driver that resolves UNC paths, reachable through Distributed File System (DFS) referral processing. A malformed referral response triggers an untrusted pointer dereference in the Windows kernel. Microsoft assigned **CVE-2026-70111** (MSRC case 126173), rated it a Windows Kernel Elevation of Privilege vulnerability, and shipped a fix in the October 2026 Security Update Release.

The bar is low: network adjacency, no privileges required. Corelight reproduced a reliable crash on demand. Microsoft's own analysis goes further: successful exploitation can grant an attacker full SYSTEM privileges.

Every currently supported Windows version is affected: Windows 10, Windows 11, and Windows Server 2012 through 2025. A single domain controller going down takes Kerberos and LDAP with it for every host in its scope until it reboots.

We found this while researching DFS-based coercion attacks. We haven't seen it exploited in the wild.

CORELIGHT COVERAGE

- Corelight Feed signatures for exploitation attempts
- Zeek `conn.log` crash-confirmation chain
- Live the same day as Microsoft's patch
- If you have Corelight, you're already covered

SEVERITY AND AFFECTED PRODUCTS

Field	Value
CVE	CVE-2026-70111
CVSS score	8.1 (High)
Impact	Elevation of Privilege, SYSTEM-level access
Affected products	Windows 10, Windows 11, Windows Server 2012 through 2025 (all currently supported versions)
Privileges required	None (network adjacency only)
Attack complexity	High, per Microsoft's assessment
Active exploitation	None observed

CORELIGHT DETECTION

If you have Corelight deployed, you're already covered:

- **Corelight Feed** signatures, part of the Open NDR Platform, that flag malformed DFS referral responses consistent with exploitation attempts.
- **Zeek `conn.log` crash-confirmation chain** that correlates connection behavior with a triggered kernel fault on the target host.

DEPLOYMENT NOTE

This detection requires east-west network visibility to fire. If you're not sure whether your deployment has proper coverage, contact your Corelight representative, they can help you check.

TIMELINE

Milestone	Detail
Proactive discovery	Corelight Research, during DFS attack-surface mapping
Reported to Microsoft	MSRC case 126173 opened
CVE assigned	CVE-2026-70111
Patch release, 2026-10-13	Fix shipped in Microsoft's October 2026 Security Update Release; Corelight detection content shipped same day

To learn more, visit

<https://corelight.com/blog/cve-2026-70111-microsoft-distributed-file-system-0-day>



Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response Platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497

Published 2026-10-13. All rights reserved. © Copyright 2026 Corelight, Inc. Windows is a trademark of Microsoft Corporation.