PowerDNS Security Advisory 2026-02 for DNSdist: Multiple issues

CVE-2026-0396: HTML injection in the web dashboard

- CVE: CVE-2026-0396
- Date: 2026-03-31T00:00:00+01:00
- Discovery date: 2025-12-19T00:00:00+01:00
- Affects: PowerDNS DNSdist from 1.9.0 to 1.9.11, from 2.0.0 to 2.0.2
- Not affected: PowerDNS DNSdist 1.9.12, 2.0.3
- Severity: Low
- Impact: HTML injection
- Exploit: This problem can be triggered by an attacker sending crafted DNS queries triggering domain-based dynamic rules
- Risk of system compromise: None
- Solution: Upgrade to patched version
- CWE: CWE-80
- CVSS: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N
- Last affected: 1.9.11,2.0.2
- First fixed: 1.9.12,2.0.3
- Internal ID: 342

An attacker might be able to inject HTML content into the internal web dashboard by sending crafted DNS queries to a DNSdist instance where domain-based dynamic rules have been enabled via either *DynBlockRulesGroup:setSuffixMatchRule* or *DynBlockRulesGroup:setSuffixMatchRuleFFI*.

CVSS Score: 3.1

The remedy is: upgrade to a patched version.

We would like to thank Aisle Research for finding and reporting the issue.

CVE-2026-0397: Information disclosure via CORS misconfiguration

- CVE: CVE-2026-0397
- Date: 2026-03-31T00:00:00+01:00
- Discovery date: 2026-01-13T00:00:00+01:00
- Affects: PowerDNS DNSdist from 1.9.0 to 1.9.11, from 2.0.0 to 2.0.2
- Not affected: PowerDNS DNSdist 1.9.12, 2.0.3
- Severity: Low
- Impact: Information disclosure
- Exploit: This problem can be triggered by an attacker tricking an administrator logged to the DNSdist's dashboard into visiting a malicious website
- Risk of system compromise: None
- Solution: Upgrade to patched version or disable the internal webserver
- CWE: CWE-942
- CVSS: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
- Last affected: 1.9.11,2.0.2
- First fixed: 1.9.12,2.0.3
- Internal ID: 344

When the internal webserver is enabled (default is disabled), an attacker might be able to trick an administrator logged to the dashboard into visiting a malicious website and extract information about the running configuration from the dashboard. The root cause of the issue is a misconfiguration of the Cross-Origin Resource Sharing (CORS) policy.

CVSS Score: 3.1

The remedy is: upgrade to a patched version, or disable the internal webserver.

We would like to thank Surya Narayan Kushwaha (aka Cavid) for finding and reporting the issue.

CVE-2026-24028: Out-of-bounds read when parsing DNS packets via Lua

- CVE: CVE-2026-24028
- Date: 2026-03-31T00:00:00+01:00
- Discovery date: 2026-02-11T00:00:00+01:00
- Affects: PowerDNS DNSdist from 1.9.0 to 1.9.11, from 2.0.0 to 2.0.2
- Not affected: PowerDNS DNSdist 1.9.12, 2.0.3
- Severity: Medium
- Impact: Denial of service or Information disclosure
- Exploit: This problem can be triggered by an attacker sending crafted DNS responses
- Risk of system compromise: None
- Solution: Upgrade to patched version or stop using newDNSPacketOverlay
- CWE: CWE-126
- CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
- Last affected: 1.9.11,2.0.2
- First fixed: 1.9.12,2.0.3
- Internal ID: 347

An attacker might be able to trigger an out-of-bounds read by sending a crafted DNS response packet, when custom Lua code uses *newDNSPacketOverlay* to parse DNS packets. The out-of-bounds read might trigger a crash, leading to a denial of service, or access unrelated memory, leading to potential information disclosure.

CVSS Score: 5.3

The remedy is: upgrade to a patched version or stop using newDNSPacketOverlay

We would like to thank Naoki Wakamatsu for finding and reporting the issue.

CVE-2026-24029: DNS over HTTPS ACL bypass

- CVE: CVE-2026-24029
- Date: 2026-03-31T00:00:00+01:00
- Discovery date: 2026-02-12T00:00:00+01:00
- Affects: PowerDNS DNSdist from 1.9.0 to 1.9.11, from 2.0.0 to 2.0.2
- Not affected: PowerDNS DNSdist 1.9.12, 2.0.3

- Severity: Medium
- Impact: ACL bypass
- Exploit: This problem can be triggered by an attacker sending DoH queries
- Risk of system compromise: None
- Solution: Upgrade to patched version or keep the *early_acl_drop* option enabled
- CWE: CWE-863
- CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
- Last affected: 1.9.11,2.0.2
- First fixed: 1.9.12,2.0.3
- Internal ID: 348

When the *early_acl_drop* (*earlyACLDrop* in Lua) option is disabled (default is enabled) on a DNS over HTTPs frontend using the *nghttp2* provider, the ACL check is skipped, allowing all clients to send DoH queries regardless of the configured ACL.

CVSS Score: 6.5

The remedy is: upgrade to a patched version or keep the *early_acl_drop* option enabled

We would like to thank Surya Narayan Kushwaha (aka Cavid) for finding and reporting the issue.

CVE-2026-24030: Unbounded memory allocation for DoQ and DoH3

- CVE: CVE-2026-24030
- Date: 2026-03-31T00:00:00+01:00
- Discovery date: 2026-02-17T00:00:00+01:00
- Affects: PowerDNS DNSdist from 1.9.0 to 1.9.11, from 2.0.0 to 2.0.2
- Not affected: PowerDNS DNSdist 1.9.12, 2.0.3
- Severity: Medium
- Impact: Denial of service
- Exploit: This problem can be triggered by an attacker sending DoQ or DoH3 queries
- Risk of system compromise: None
- Solution: Upgrade to patched version

- CWE: CWE-789
- CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
- Last affected: 1.9.11,2.0.2
- First fixed: 1.9.12,2.0.3
- Internal ID: 359

An attacker might be able to trick DNSdist into allocating too much memory while processing DNS over QUIC or DNS over HTTP/3 payloads, resulting in a denial of service. In setups with a large quantity of memory available this usually results in an exception and the QUIC connection is properly closed, but in some cases the system might enter an out-of-memory state instead and terminate the process.

CVSS Score: 5.3

The remedy is: upgrade to a patched version

We would like to thank XavLimSG for finding and reporting the issue.

CVE-2026-27854: Use after free when parsing EDNS options in Lua

- CVE: CVE-2026-27854
- Date: 2026-03-31T00:00:00+01:00
- Discovery date: 2026-02-22T00:00:00+01:00
- Affects: PowerDNS DNSdist from 1.9.0 to 1.9.11, from 2.0.0 to 2.0.2
- Not affected: PowerDNS DNSdist 1.9.12, 2.0.3
- Severity: Medium
- Impact: Denial of service
- Exploit: This problem can be triggered by an attacker sending crafted DNS queries in very specific setups
- Risk of system compromise: None
- Solution: Upgrade to patched version or do not use DNSQuestion:getEDNSOptions
- CWE: CWE-416
- CVSS: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L

- Last affected: 1.9.11,2.0.2
- First fixed: 1.9.12,2.0.3
- Internal ID: 362

An attacker might be able to trigger a use-after-free by sending crafted DNS queries to a DNSdist using the DNSQuestion:getEDNSOptions method in custom Lua code. In some cases DNSQuestion:getEDNSOptions might refer to a version of the DNS packet that has been modified, thus triggering a use-after-free and potentially a crash resulting in denial of service.

CVSS Score: 4.8

The remedy is: upgrade to a patched version or do not use DNSQuestion:getEDNSOptions

We would like to thank Naoki Wakamatsu for finding and reporting the issue.

CVE-2026-27853: Out-of-bounds write when rewriting large DNS packets

- CVE: CVE-2026-27853
- Date: 2026-03-31T00:00:00+01:00
- Discovery date: 2026-03-04T00:00:00+01:00
- Affects: PowerDNS DNSdist from 1.9.0 to 1.9.11, from 2.0.0 to 2.0.2
- Not affected: PowerDNS DNSdist 1.9.12, 2.0.3
- Severity: Medium
- Impact: Denial of service
- Exploit: This problem can be triggered by an attacker sending crafted DNS responses in very specific setups
- Risk of system compromise: None
- Solution: Upgrade to patched version or do not use DNSQuestion:changeName or DNSResponse:changeName
- CWE: CWE-416
- CVSS: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
- Last affected: 1.9.11,2.0.2
- First fixed: 1.9.12,2.0.3

- Internal ID: 372

An attacker might be able to trigger an out-of-bounds write by sending crafted DNS responses to a DNSdist using the DNSQuestion:changeName or DNSResponse:changeName methods in custom Lua code. In some cases the rewritten packet might become larger than the initial response and even exceed 65535 bytes, potentially leading to a crash resulting in denial of service.

CVSS Score: 5.9

The remedy is: upgrade to a patched version or do not use DNSQuestion:changeName or DNSResponse:changeName.

We would like to thank ilya rozentsvaig for finding and reporting the issue.