PowerDNS Security Advisory 2026-04 for DNSdist: Multiple issues

CVE-2026-33257: Insufficient input validation of internal webserver

- CVE: CVE-2026-33257
- Date: 2026-04-22T00:00:00+01:00
- Discovery date: 2026-02-16T00:00:00+01:00
- Affects: PowerDNS DNSdist up to and including 2.0.3 and 1.9.12
- Not affected: PowerDNS DNSdist 1.9.13, 2.0.4
- Severity: Medium
- Impact: Denial of service
- Exploit: This problem can be triggered by an attacker sending crafted http requests, but only if the internal webserver is enabled.
- Risk of system compromise: None
- Solution: Upgrade to patched version or disallow network access to web server
- CWE: CWE-770
- CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
- Last affected: 1.9.12,2.0.3
- First fixed: 1.9.13,2.0.4
- Internal ID: 368

An attacker can send a web request that causes unlimited memory allocation in the internal web server, leading to a denial of service. The internal web server is disabled by default.

`https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L`__

The remedy is: upgrade to a patched version, or prevent network access to the internal webserver. In general for defense in-depth reasons we recommend making the internal web server only

accessible to trusted clients.

We would like to thank Vitaly Simonovich for bringing this issue to our attention.

CVE-2026-33260: Insufficient input validation of internal webserver

- CVE: CVE-2026-33260
- Date: 2026-04-22T00:00:00+01:00
- Discovery date: 2026-02-20T00:00:00+01:00
- Affects: PowerDNS DNSdist up to and including 2.0.3 and 1.9.12
- Not affected: PowerDNS DNSdist 1.9.13, 2.0.4
- Severity: Medium
- Impact: Denial of service
- Exploit: This problem can be triggered by an attacker sending crafted http requests, but only if the internal webserver is enabled.
- Risk of system compromise: None
- Solution: Upgrade to patched version or disallow network access to web server
- CWE: CWE-770
- CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
- Last affected: 1.9.12,2.0.3
- First fixed: 1.9.13,2.0.4
- Internal ID: 374

An attacker can send a web request that causes unlimited memory allocation in the internal web server, leading to a denial of service. The internal web server is disabled by default.

`https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L`__

The remedy is: upgrade to a patched version, or prevent network access to the internal webserver. In general for defense in-depth reasons we recommend making the internal web server only accessible to trusted clients.

We would like to thank Cavid for bringing this issue to our attention.

CVE-2026-33254: Resource exhaustion via DoQ/DoH3 connections

- CVE: CVE-2026-33254
- Date: 2026-04-22T00:00:00+01:00
- Discovery date: 2026-03-15T00:00:00+01:00
- Affects: PowerDNS DNSdist up to and including 2.0.3 and 1.9.12
- Not affected: PowerDNS DNSdist 1.9.13, 2.0.4
- Severity: Medium
- Impact: Denial of service
- Exploit: This problem can be triggered by an attacker opening a large number of DoQ or DoH3 connections
- Risk of system compromise: None
- Solution: Upgrade to patched version or do not enable DoQ or DoH3
- CWE: CWE-770
- CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
- Last affected: 1.9.12,2.0.3
- First fixed: 1.9.13,2.0.4
- Internal ID: 385

An attacker can create a large number of concurrent DoQ or DoH3 connections, causing unlimited memory allocation in DNSdist and leading to a denial of service. DOQ and DoH3 are disabled by default.

`https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L`__

The remedy is: upgrade to a patched version, or do not enable DoQ or DoH3.

We would like to thank Salvor Labs - https://salvor.fr for bringing this issue to our attention.

CVE-2026-33602: Off-by-one access when processing crafted UDP responses

- CVE: CVE-2026-33602
- Date: 2026-04-22T00:00:00+01:00
- Discovery date: 2026-03-23T00:00:00+01:00
- Affects: PowerDNS DNSdist up to and including 2.0.3 and 1.9.12
- Not affected: PowerDNS DNSdist 1.9.13, 2.0.4
- Severity: High
- Impact: Denial of service
- Exploit: This problem can be triggered by a rogue backend sending crafted UDP responses
- Risk of system compromise: None
- Solution: Upgrade to patched version
- CWE: CWE-122
- CVSS: 3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H
- Last affected: 1.9.12,2.0.3
- First fixed: 1.9.13,2.0.4
- Internal ID: 402

A rogue backend can send a crafted UDP response with a query ID off by one related to the maximum configured value, triggering an out-of-bounds write leading to a denial of service.

`https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H`__

The remedy is: upgrade to a patched version.

We would like to thank ylwango613 for bringing this issue to our attention.

CVE-2026-33599: Out-of-bounds read in service discovery

- CVE: CVE-2026-33599
- Date: 2026-04-22T00:00:00+01:00
- Discovery date: 2026-03-25T00:00:00+01:00
- Affects: PowerDNS DNSdist up to and including 2.0.3 and 1.9.12
- Not affected: PowerDNS DNSdist 1.9.13, 2.0.4

- Severity: Low
- Impact: Denial of service
- Exploit: This problem can be triggered by a rogue backend sending crafted SVCB responses
- Risk of system compromise: None
- Solution: Upgrade to patched version or do not enable DDR
- CWE: CWE-125
- CVSS: 3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
- Last affected: 1.9.12,2.0.3
- First fixed: 1.9.13,2.0.4
- Internal ID: 420

A rogue backend can send a crafted SVCB response to a Discovery of Designated Resolvers request, when requested via either the autoUpgrade (Lua) option to newServer or auto_upgrade (YAML) settings. DDR upgrade is not enabled by default.

`https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L`__

The remedy is: upgrade to a patched version or do not enable DDR.

We would like to thank ylwango613 for bringing this issue to our attention.

CVE-2026-33598: Out-of-bounds read in cache inspection via Lua

- CVE: CVE-2026-33598
- Date: 2026-04-22T00:00:00+01:00
- Discovery date: 2026-03-26T00:00:00+01:00
- Affects: PowerDNS DNSdist up to and including 2.0.3 and 1.9.12
- Not affected: PowerDNS DNSdist 1.9.13, 2.0.4
- Severity: Low
- Impact: Denial of service
- Exploit: This problem can be triggered by a crafted response
- Risk of system compromise: None

- Solution: Upgrade to patched version or do not use getDomainListByAddress or getAddressListByDomain
- CWE: CWE-125
- CVSS: 3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L
- Last affected: 1.9.12,2.0.3
- First fixed: 1.9.13,2.0.4
- Internal ID: 421

A cached crafted response can cause an out-of-bounds read if custom Lua code calls getDomainListByAddress() or getAddressListByDomain() on a packet cache.

`https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L`__

The remedy is: upgrade to a patched version or getDomainListByAddress or getAddressListByDomain.

We would like to thank ylwango613 for bringing this issue to our attention.

CVE-2026-33597: PRSD detection denial of service

- CVE: CVE-2026-33597
- Date: 2026-04-22T00:00:00+01:00
- Discovery date: 2026-03-26T00:00:00+01:00
- Affects: PowerDNS DNSdist up to and including 2.0.3 and 1.9.12
- Not affected: PowerDNS DNSdist 1.9.13, 2.0.4
- Severity: Low
- Impact: Denial of service
- Exploit: This problem can be triggered by a crafted query
- Risk of system compromise: None
- Solution: Upgrade to patched version
- CWE: CWE-116
- CVSS: 3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
- Last affected: 1.9.12,2.0.3

- First fixed: 1.9.13,2.0.4
- Internal ID: 422

A crafted query containing an invalid DNS label can prevent the PRSD detection algorithm executed via DynBlockRulesGroup:setSuffixMatchRule or DynBlockRulesGroup:setSuffixMatchRuleFFI from being executed.

`https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L`__

The remedy is: upgrade to a patched version.

We would like to thank Mehtab Zafar for bringing this issue to our attention.

CVE-2026-33596: TCP backend stream ID overflow

- CVE: CVE-2026-33596
- Date: 2026-04-22T00:00:00+01:00
- Discovery date: 2026-03-26T00:00:00+01:00
- Affects: PowerDNS DNSdist up to and including 2.0.3 and 1.9.12
- Not affected: PowerDNS DNSdist 1.9.13, 2.0.4
- Severity: Low
- Impact: Denial of service
- Exploit: This problem can be triggered by a client sending perfectly timed queries routed to a TCP-only or DoT backend
- Risk of system compromise: None
- Solution: Upgrade to patched version
- CWE: CWE-190
- CVSS: 3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
- Last affected: 1.9.12,2.0.3
- First fixed: 1.9.13,2.0.4
- Internal ID: 423

A client might theoretically be able to cause a mismatch between queries sent to a backend and the received responses by sending a flood of perfectly timed queries that are routed to a TCP-only

or DNS over TLS backend.

`https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L`__

The remedy is: upgrade to a patched version.

We would like to thank ylwango613 for bringing this issue to our attention.

CVE-2026-33595: DoQ/DoH3 excessive memory allocation

- CVE: CVE-2026-33595
- Date: 2026-04-22T00:00:00+01:00
- Discovery date: 2026-03-28T00:00:00+01:00
- Affects: PowerDNS DNSdist up to and including 2.0.3 and 1.9.12
- Not affected: PowerDNS DNSdist 1.9.13, 2.0.4
- Severity: Medium
- Impact: Denial of service
- Exploit: This problem can be triggered by a client generating a big amount of errors over a DoQ or DoH3 connection
- Risk of system compromise: None
- Solution: Upgrade to patched version or disable DoQ and DoH3
- CWE: CWE-770
- CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
- Last affected: 1.9.12,2.0.3
- First fixed: 1.9.13,2.0.4
- Internal ID: 451

A client can trigger excessive memory allocation by generating a lot of errors responses over a single DoQ and DoH3 connection, as some resources were not properly released until the end of the connection.

`https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L`__

The remedy is: upgrade to a patched version or disable DoQ or DoH3.

We would like to thank Mehtab Zafar for bringing this issue to our attention.

CVE-2026-33594: Outgoing DoH excessive memory allocation

- CVE: CVE-2026-33594
- Date: 2026-04-22T00:00:00+01:00
- Discovery date: 2026-03-28T00:00:00+01:00
- Affects: PowerDNS DNSdist up to and including 2.0.3 and 1.9.12
- Not affected: PowerDNS DNSdist 1.9.13, 2.0.4
- Severity: Medium
- Impact: Denial of service
- Exploit: This problem can be triggered by a client generating a lot of queries routed to an overloaded DoH backend
- Risk of system compromise: None
- Solution: Upgrade to patched version or disable outgoing DoH
- CWE: CWE-770
- CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
- Last affected: 1.9.12,2.0.3
- First fixed: 1.9.13,2.0.4
- Internal ID: 452

A client can trigger excessive memory allocation by generating a lot of queries that are routed to an overloaded DoH backend, causing queries to accumulate into a buffer that will not be released until the end of the connection.

`https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L`__

The remedy is: upgrade to a patched version or disable outgoing DoH.

We would like to thank Mehtab Zafar for bringing this issue to our attention.

CVE-2026-33593: Denial of service via crafted DNSCrypt query

- CVE: CVE-2026-33593
- Date: 2026-04-22T00:00:00+01:00
- Discovery date: 2026-04-03T00:00:00+01:00
- Affects: PowerDNS DNSdist up to and including 2.0.3 and 1.9.12
- Not affected: PowerDNS DNSdist 1.9.13, 2.0.4
- Severity: High
- Impact: Denial of service
- Exploit: This problem can be triggered by a client sending a crafted DNSCrypt query
- Risk of system compromise: None
- Solution: Upgrade to patched version or disable DNSCrypt
- CWE: CWE-369
- CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- Last affected: 1.9.12,2.0.3
- First fixed: 1.9.13,2.0.4
- Internal ID: 458

A client can trigger a divide by zero error leading to crash by sending a crafted DNSCrypt query.

`https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H`__

The remedy is: upgrade to a patched version or disable DNSCrypt.

We would like to thank Haruto Kimura (Stella) for bringing this issue to our attention.