



CVE-2009-3602

Published on: 10/13/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:25 PM UTC

CVE-2009-3602

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Unbound](#) from [Nlnetlabs](#) contain the following vulnerability:

Unbound before 1.3.4 does not properly verify signatures for NSEC3 records, which allows remote attackers to cause secure delegations to be downgraded via DNS spoofing or other DNS-related attacks in conjunction with crafted delegation responses.

CVE-2009-3602 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

oss-security - Re: CVE request: Unbound

www.openwall.com
text/html

[MLIST \[oss-security\]
20091009 Re: CVE request:
Unbound](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[Vendor Advisory](#)
www.vupen.com
text/html

[VUPEN ADV-2009-2875](#)

Unbound NSEC3 Signature Validation Bypass Security Issue - Secunia
Advisories - Vulnerability Information - Secunia.com

[Vendor Advisory](#)
web.archive.org
text/html

[SECUNIA 36996](#)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
text/html

[XF unbound-nsec3-
security-bypass\(53729\)](#)

[Unbound-users] Release of unbound 1.3.4

[Vendor Advisory](#)
unbound.net

[MLIST \[Unbound-users\]
20091007 Release of](#)

[text/html](#)[unbound 1.3.4](#)

Debian update for unbound - Secunia.com

[web.archive.org](#)[SECUNIA 37913](#)[text/html](#)

No Description Provided

[osvdb.org](#)[OSVDB 58836](#)[Inactive Link](#)[Not Archived](#)

oss-security - CVE request: Unbound

[www.openwall.com](#)[MLIST \[oss-security\]
20091009 CVE request:
Unbound](#)[text/html](#)

Debian -- Security Information -- DSA-1963-1 unbound

[www.debian.org](#)[DEBIAN DSA-1963](#)[Deprecated Link](#)[text/html](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nlnetlabs	Unbound	0.0	All	All	All
Application	Nlnetlabs	Unbound	0.09	All	All	All
Application	Nlnetlabs	Unbound	0.1	All	All	All
Application	Nlnetlabs	Unbound	0.10	All	All	All
Application	Nlnetlabs	Unbound	0.11	All	All	All
Application	Nlnetlabs	Unbound	0.2	All	All	All
Application	Nlnetlabs	Unbound	0.3	All	All	All
Application	Nlnetlabs	Unbound	0.4	All	All	All
Application	Nlnetlabs	Unbound	0.5	All	All	All
Application	Nlnetlabs	Unbound	0.6	All	All	All
Application	Nlnetlabs	Unbound	0.7	All	All	All
Application	Nlnetlabs	Unbound	0.7.1	All	All	All
Application	Nlnetlabs	Unbound	0.7.2	All	All	All
Application	Nlnetlabs	Unbound	0.8	All	All	All
Application	Nlnetlabs	Unbound	1.0.0	All	All	All
Application	Nlnetlabs	Unbound	1.0.1	All	All	All
Application	Nlnetlabs	Unbound	1.0.2	All	All	All
Application	Nlnetlabs	Unbound	1.1.0	All	All	All
Application	Nlnetlabs	Unbound	1.1.1	All	All	All

Application	Nlnetlabs	Unbound	1.2.0	All	All	All
Application	Nlnetlabs	Unbound	1.2.1	All	All	All
Application	Nlnetlabs	Unbound	1.3.0	All	All	All
Application	Nlnetlabs	Unbound	1.3.1	All	All	All
Application	Nlnetlabs	Unbound	1.3.2	All	All	All
Application	Nlnetlabs	Unbound	0.0	All	All	All
Application	Nlnetlabs	Unbound	0.09	All	All	All
Application	Nlnetlabs	Unbound	0.1	All	All	All
Application	Nlnetlabs	Unbound	0.10	All	All	All
Application	Nlnetlabs	Unbound	0.11	All	All	All
Application	Nlnetlabs	Unbound	0.2	All	All	All
Application	Nlnetlabs	Unbound	0.3	All	All	All
Application	Nlnetlabs	Unbound	0.4	All	All	All
Application	Nlnetlabs	Unbound	0.5	All	All	All
Application	Nlnetlabs	Unbound	0.6	All	All	All
Application	Nlnetlabs	Unbound	0.7	All	All	All
Application	Nlnetlabs	Unbound	0.7.1	All	All	All
Application	Nlnetlabs	Unbound	0.7.2	All	All	All
Application	Nlnetlabs	Unbound	0.8	All	All	All
Application	Nlnetlabs	Unbound	1.0.0	All	All	All
Application	Nlnetlabs	Unbound	1.0.1	All	All	All
Application	Nlnetlabs	Unbound	1.0.2	All	All	All
Application	Nlnetlabs	Unbound	1.1.0	All	All	All
Application	Nlnetlabs	Unbound	1.1.1	All	All	All
Application	Nlnetlabs	Unbound	1.2.0	All	All	All
Application	Nlnetlabs	Unbound	1.2.1	All	All	All
Application	Nlnetlabs	Unbound	1.3.0	All	All	All
Application	Nlnetlabs	Unbound	1.3.1	All	All	All
Application	Nlnetlabs	Unbound	1.3.2	All	All	All
Application	Nlnetlabs	Unbound	All	All	All	All
cpe:2.3:a:nlnetlabs:unbound:0.0:*****:						
cpe:2.3:a:nlnetlabs:unbound:0.09:*****:						
cpe:2.3:a:nlnetlabs:unbound:0.1:*****:						
cpe:2.3:a:nlnetlabs:unbound:0.10:*****:						

cpe:2.3:a:nlnetlabs:unbound:0.11:*:*:*:*:*:*:

```
cpe:2.3:a:nlnetlabs:unbound:0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:0.3:*:*:*:*:*:*:
```

cpe:2.3:a:nlnetlabs:unbound:0.4:*:*:*:*:*:

cpe:2.3:a:nlnetlabs:unbound:0.5.*:*:*:*:*:*:

```
cpe:2.3:a:nlnetlabs:unbound:0.6.*:*:*:*:*:*:
```

cpe:2.3:a:nlnetlabs:unbound:0.7:*:*:*:*:*:*:

cpe:2.3:a:nlnetlabs:unbound:0.7.1:*:*:*:*:*:*:

```
cpe:2.3:a:nlnetlabs:unbound:0.7.2:*:*:*:*:*:*:
```

cpe:2.3:a:nlnetlabs:unbound:0.8:*:*:*:*:*:*:

```
cpe:2.3:a:nlnetlabs:unbound:1.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:1.0.1:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:nlnetlabs:unbound:1.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:1.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:1.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:1.2.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:1.2.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:1.3.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:1.3.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:1.3.2:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:0.0.*:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:0.9:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:0.1:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:0.10:*.:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:0.11:.*:.*:.*:.*:.*:.*:.*
```

cpe:2.3:a:nlnetlabs:unbound:0.2:*:*:*:*:*:

```
cpe:2.3:a:nlnetlabs:unbound:0.3:*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:0.4.*:*:*:*:*:
```

```
cpe:2.3:a:nlnetlabs:unbound:0.5:*:*:*:*:*:
```

cpe:2.3:a:nlnetlabs:unbound:0.6:*****:
cpe:2.3:a:nlnetlabs:unbound:0.7:*****:
cpe:2.3:a:nlnetlabs:unbound:0.7.1:*****:
cpe:2.3:a:nlnetlabs:unbound:0.7.2:*****:
cpe:2.3:a:nlnetlabs:unbound:0.8:*****:
cpe:2.3:a:nlnetlabs:unbound:1.0.0:*****:
cpe:2.3:a:nlnetlabs:unbound:1.0.1:*****:
cpe:2.3:a:nlnetlabs:unbound:1.0.2:*****:
cpe:2.3:a:nlnetlabs:unbound:1.1.0:*****:
cpe:2.3:a:nlnetlabs:unbound:1.1.1:*****:
cpe:2.3:a:nlnetlabs:unbound:1.2.0:*****:
cpe:2.3:a:nlnetlabs:unbound:1.2.1:*****:
cpe:2.3:a:nlnetlabs:unbound:1.3.0:*****:
cpe:2.3:a:nlnetlabs:unbound:1.3.1:*****:
cpe:2.3:a:nlnetlabs:unbound:1.3.2:*****:
cpe:2.3:a:nlnetlabs:unbound:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)