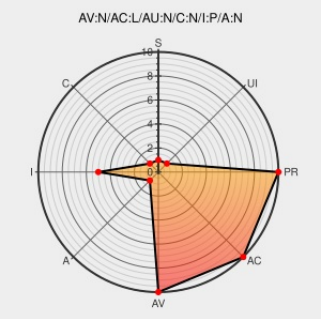
CVE-2002-2212

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:04 PM UTC

CVE-2002-2212

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Uxp V from Fujitsu contain the following vulnerability:

The DNS resolver in unspecified versions of Fujitsu UXP/V, when resolving recursive DNS queries for arbitrary hosts, allows remote attackers to conduct DNS cache poisoning via a birthday attack that uses a large number of open queries for the same resource record (RR) combined with spoofed responses, which increases the possibility of successfully spoofing a response in a way that is more efficient than brute force methods.

CVE-2002-2212 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Fujitsu Information for VU#457875	www.kb.cert.org text/html	CONFIRM www.kb.cert.org/vuls/id/IAFY-5FDT5K
A página não foi encontrada	Patch web.archive.org text/html Inactive Link Not Archived	MISC www.rnp.br/cais/alertas/2002/cais-ALR-19112002a.html
Spiral Bound - The Most Informative Website About Internet Network	www.imconf.net application/pdf	MISC www.imconf.net/imw-2002/imw2002-papers/198.pdf
CERT/CC Vulnerability Note VU#457875	US Government Resource www.kb.cert.org text/html	CERT-VN VU#457875

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
Hardware	Fujitsu	Uxp V	All	All	All	All
Hardware	Fujitsu	Uxp V	All	All	All	All
Application	Isc	Bind	4.9	All	All	All
Application	Isc	Bind	4.9.10	All	All	All
Application	Isc	Bind	4.9.2	All	All	All
Application	Isc	Bind	4.9.3	All	All	All
Application	Isc	Bind	4.9.4	All	All	All
Application	Isc	Bind	4.9.5	All	All	All
Application	Isc	Bind	4.9.5	p1	All	All
Application	Isc	Bind	4.9.6	All	All	All
Application	Isc	Bind	4.9.7	All	All	All
Application	Isc	Bind	4.9.8	All	All	All
Application	Isc	Bind	4.9.9	All	All	All
Application	Isc	Bind	8.2	All	All	All
Application	Isc	Bind	8.2.1	All	All	All
Application	Isc	Bind	8.2.2	All	All	All
Application	Isc	Bind	8.2.2	p1	All	All
Application	Isc	Bind	8.2.2	p2	All	All
Application	Isc	Bind	8.2.2	p3	All	All
Application	Isc	Bind	8.2.2	p4	All	All
Application	Isc	Bind	8.2.2	p5	All	All
Application	Isc	Bind	8.2.2	p6	All	All
Application	Isc	Bind	8.2.2	p7	All	All
Application	Isc	Bind	8.2.3	All	All	All
Application	Isc	Bind	8.2.4	All	All	All
Application	Isc	Bind	8.2.5	All	All	All
Application	Isc	Bind	8.2.6	All	All	All

Application	Isc	Bind	8.2.7	All	All	All
Application	Isc	Bind	8.3.0	All	All	All
Application	Isc	Bind	8.3.1	All	All	All
Application	Isc	Bind	8.3.2	All	All	All
Application	Isc	Bind	8.3.3	All	All	All
Application	Isc	Bind	8.3.4	All	All	All
Application	Isc	Bind	4.9	All	All	All
Application	Isc	Bind	4.9.10	All	All	All
Application	Isc	Bind	4.9.2	All	All	All
Application	Isc	Bind	4.9.3	All	All	All
Application	Isc	Bind	4.9.4	All	All	All
Application	Isc	Bind	4.9.5	All	All	All
Application	Isc	Bind	4.9.5	p1	All	All
Application	Isc	Bind	4.9.6	All	All	All
Application	Isc	Bind	4.9.7	All	All	All
Application	Isc	Bind	4.9.8	All	All	All
Application	Isc	Bind	4.9.9	All	All	All
Application	Isc	Bind	8.2	All	All	All
Application	Isc	Bind	8.2.1	All	All	All
Application	Isc	Bind	8.2.2	All	All	All
Application	Isc	Bind	8.2.2	p1	All	All
Application	Isc	Bind	8.2.2	p2	All	All
Application	Isc	Bind	8.2.2	p3	All	All
Application	Isc	Bind	8.2.2	p4	All	All
Application	Isc	Bind	8.2.2	p5	All	All
Application	Isc	Bind	8.2.2	p6	All	All
Application	Isc	Bind	8.2.2	p7	All	All
Application	Isc	Bind	8.2.3	All	All	All
Application	Isc	Bind	8.2.4	All	All	All
Application	Isc	Bind	8.2.5	All	All	All
Application	Isc	Bind	8.2.6	All	All	All
Application	Isc	Bind	8.2.7	All	All	All
Application	Isc	Bind	8.3.0	All	All	All
Application	Isc	Bind	8.3.1	All	All	All
Application	Isc	Bind	8.3.2	All	All	All

Application	Isc	Bind	8.3.3	All	All	All
Application	Isc	Bind	8.3.4	All	All	All

- cpe:2.3:h:fujitsu:uxp_v:*:*:*:*:*:*:*:*:
- cpe:2.3:h:fujitsu:uxp_v:*:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:4.9:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:4.9.10:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:4.9.2:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:4.9.3:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:4.9.4:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:4.9.5:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:4.9.5:p1:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:4.9.6:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:4.9.7:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:4.9.8:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:4.9.9:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.1:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.2:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.2:p1:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.2:p2:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.2:p3:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.2:p4:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.2:p5:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.2:p6:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.2:p7:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.3:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.4:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.5:*:*:*:*:*:*:*:
- cpe:2.3:a:isc:bind:8.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:4.9:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:4.9.10:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:4.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:4.9.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:4.9.4:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:4.9.5:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:4.9.5:p1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:4.9.6:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:4.9.7:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:4.9.8:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:4.9.9:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.2:p1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.2:p2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.2:p3:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.2:p4:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.2:p5:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.2:p6:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.2:p7:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:8.2.4:*:*:*:*:*:*:*

cpe:2.3:a:isc:bind:8.2.5:*:*:*:*:*:*:*

cpe:2.3:a:isc:bind:8.2.6:*:*:*:*:*:*:*

cpe:2.3:a:isc:bind:8.2.7:*:*:*:*:*:*:*

cpe:2.3:a:isc:bind:8.3.0:*:*:*:*:*:*:*

cpe:2.3:a:isc:bind:8.3.1:*:*:*:*:*:*:*

cpe:2.3:a:isc:bind:8.3.2:*:*:*:*:*:*:*

cpe:2.3:a:isc:bind:8.3.3:*:*:*:*:*:*:*

cpe:2.3:a:isc:bind:8.3.4:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→