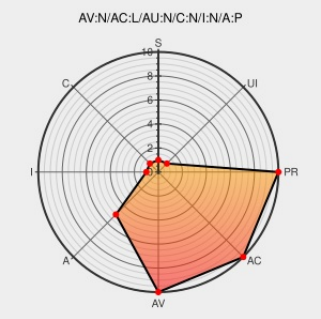
# CVE-2002-0601

Published on: 06/18/2002 04:00:00 AM UTC

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

## CVE-2002-0601

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




Certain versions of Realsecure Network Sensor from Information Security Systems contain the following vulnerability:

ISS RealSecure Network Sensor 5.x through 6.5 allows remote attackers to cause a denial of service (crash) via malformed DHCP packets that cause RealSecure to dereference a null pointer.

CVE-2002-0601 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 | NONE | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Neohapsis Archives - Bugtraq - ISS Advisory: Remote Denial of Service Vulnerability in RealSecure Network Sensor - From xforce@iss.net | Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived | BUGTRAQ 20020430 ISS Advisory: Remote Denial of Service Vulnerability in RealSecure Network Sensor |
| ISS X-Force Database: rs-ns-dhcp-dos (8961): RealSecure Network Sensor DHCP denial of service | web.archive.org, text/html, Inactive Link, Not Archived | XF rs-ns-dhcp-dos(8961) |
| ISS RealSecure DHCP Signature Remote Denial Of Service Vulnerability | Patch, Vendor Advisory, cve.report (archive), text/html | BID 4649 |
| ISS: Security Center: X-Force Alerts and Advisories | Vendor Advisory, web.archive.org, text/html | ISS 20020430 Remote Denial of Service Vulnerability in RealSecure Network Sensor |

Inactive Link Not Archived

No Description Provided | www.osvdb.org | OSVDB 5165

Inactive Link Not Archived

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 | Information Security Systems | Realsecure Network Sensor | 5.0_xpu_3.4 | All | All | All |
| Application | Information Security Systems | Realsecure Network Sensor | 5.5.1_xpu_3.4 | All | All | All |
| Application | Information Security Systems | Realsecure Network Sensor | 5.5.2_xpu_3.4 | All | All | All |
| Application | Information Security Systems | Realsecure Network Sensor | 5.5_xpu_3.4 | All | All | All |
| Application | Information Security Systems | Realsecure Network Sensor | 6.0_xpu_3.4 | All | All | All |
| Application | Information Security Systems | Realsecure Network Sensor | 6.5 | All | All | All |
| Application | Information Security Systems | Realsecure Network Sensor | 5.0_xpu_3.4 | All | All | All |
| Application | Information Security Systems | Realsecure Network Sensor | 5.5.1_xpu_3.4 | All | All | All |
| Application | Information Security Systems | Realsecure Network Sensor | 5.5.2_xpu_3.4 | All | All | All |
| Application | Information Security Systems | Realsecure Network Sensor | 5.5_xpu_3.4 | All | All | All |
| Application | Information Security Systems | Realsecure Network Sensor | 6.0_xpu_3.4 | All | All | All |
| Application | Information Security Systems | Realsecure Network Sensor | 6.5 | All | All | All |

cpe:2.3:a:information_security_systems:realsecure_network_sensor:5.0_xpu_3.4:*:*:*:*:*:*:*:

cpe:2.3:a:information_security_systems:realsecure_network_sensor:5.5.1_xpu_3.4:*:*:*:*:*:*:*:

cpe:2.3:a:information_security_systems:realsecure_network_sensor:5.5.2_xpu_3.4:*:*:*:*:*:*:*:

cpe:2.3:a:information_security_systems:realsecure_network_sensor:5.5_xpu_3.4:*:*:*:*:*:*:*:

cpe:2.3:a:information_security_systems:realsecure_network_sensor:6.0_xpu_3.4:*:*:*:*:*:*:*:

cpe:2.3:a:information_security_systems:realsecure_network_sensor:6.5:*:*:*:*:*:*:*:

cpe:2.3:a:information_security_systems:realsecure_network_sensor:5.0_xpu_3.4:*:*:*:*:*:*:*:

cpe:2.3:a:information_security_systems:realsecure_network_sensor:5.5.1_xpu_3.4:*:*:*:*:*:*:*:

cpe:2.3:a:information_security_systems:realsecure_network_sensor:5.5.2_xpu_3.4:*:*:*:*:*:*:*:

cpe:2.3:a:information_security_systems:realsecure_network_sensor:5.5_xpu_3.4:*:*:*:*:*:*:*:

cpe:2.3:a:information_security_systems:realsecure_network_sensor:6.0_xpu_3.4:*:*:*:*:*:*:*:

cpe:2.3:a:information_security_systems:realsecure_network_sensor:6.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→