



CVE-2005-0455

Published on: 03/02/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:27 PM UTC

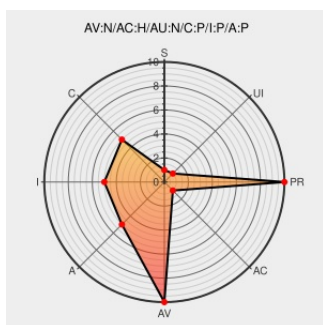
CVE-2005-0455

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Realone Player](#) from [Realnetworks](#) contain the following vulnerability:

Stack-based buffer overflow in the CSmil1Parser::testAttributeFailed function in smlparse.cpp for RealNetworks RealPlayer 10.5 (6.0.12.1056 and earlier), 10, 8, and RealOne Player V2 and V1 allows remote attackers to execute arbitrary code via a .SMIL file with a large system-screen-size value.

CVE-2005-0455 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.1 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

rhn.redhat.com | Red Hat Support

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

[REDHAT RHSA-2005:265](#)

Repository / Oval Repository

oval.cisecurity.org
[text/html](#)

[OVAL oval:org.mitre.oval:def:10926](https://oval.cisecurity.org)

Accenture | Let there be change

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

[IDeFENSE 20050301 RealNetworks RealPlayer .smil Buffer Overflow Vulnerability](#)

rhn.redhat.com | Red Hat Support

www.redhat.com
[text/html](#)

[REDHAT RHSA-2005:271](#)

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	Realnetworks	Realone Player	1.0	All	All	All
Application	Realnetworks	Realone Player	2.0	All	All	All
Application	Realnetworks	Realone Player	1.0	All	All	All
Application	Realnetworks	Realone Player	2.0	All	All	All
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.0_6.0.12.690	All	All	All
Application	Realnetworks	Realplayer	10.0_beta	All	All	All
Application	Realnetworks	Realplayer	10.5	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1016_beta	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1040	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1053	All	All	All
Application	Realnetworks	Realplayer	8.0	All	All	All
Application	Realnetworks	Realplayer	8.0	All	win32	All
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.0_6.0.12.690	All	All	All
Application	Realnetworks	Realplayer	10.0_beta	All	All	All
Application	Realnetworks	Realplayer	10.5	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1016_beta	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1040	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1053	All	All	All
Application	Realnetworks	Realplayer	8.0	All	All	All
Application	Realnetworks	Realplayer	8.0	All	win32	All

cpe:2.3:a:realnetworks:realone_player:1.0:*:*:*:*:*:

cpe:2.3:a:realnetworks:realone_player:2.0:*:*:*:*:*:

```
cpe:2.3:a:realnetworks:realone_player:1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:realnetworks:realone_player:2.0:*:*:*:*:*:*
```

```
cpe:2.3:a:realnetworks:realplayer:10.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:realnetworks:realplayer:10.0 6.0.12.690:*:*:*:*:*.*
```

```
cpe:2.3:a:realnetworks:realplayer:10.0_beta:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:realnetworks:realplayer:10.5:*:*:*:*:*:
```

```
cpe:2.3:a:realnetworks:realplayer:10.5 6.0.12.1016 beta:*:*:*:*:*:
```

```
cpe:2.3:a:realnetworks:realplayer:10.5 6.0.12.1040:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:realnetworks:realplayer:10.5 6.0.12.1053:*.~*~*~*~*~*~*
```

cpe:2.3:a:realnetworks:realplayer:8.0:*:*:*:*:*:*

```
cpe:2.3:a:realnetworks:realplayer:8.0:*:win32:*:*:*:*:*
```

```
cpe:2.3:a:realnetworks:realplayer:10.0:*:*:*:*:*:
```

```
cpe:2.3:a:realnetworks:realplayer:10.0 6.0.12.690:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:realnetworks:realplayer:10.0_beta:*:*:*:*:*.*
```

```
cpe:2.3:a:realnetworks:realplayer:10.5:*:*:*:*:*:
```

```
cpe:2.3:a:realnetworks:realplayer:10.5 6.0.12.1016 beta:*:*:*:*:*:
```

```
cpe:2.3:a:realnetworks:realplayer:10.5 6.0.12.1040:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:realnetworks:realplayer:10.5 6.0.12.1053:*.***.***.***.*
```

```
cpe:2.3:a:realnetworks:realplayer:8.0:*.:*:*:*:*:
```

```
cpe:2.3:a:realnetworks:realplayer:8.0:*:win32:*:*:*:*:*
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report