



CVE-2004-2552

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

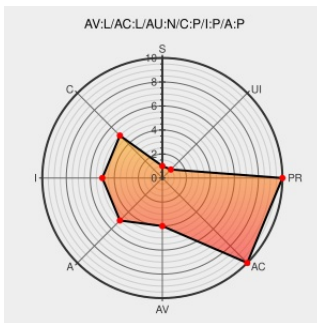
CVE-2004-2552

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Xboard](#) from [Tim Mann](#) contain the following vulnerability:

Buffer overflow in XBoard 4.2.7 and earlier might allow local users to execute arbitrary code via a long -icshost command line argument. NOTE: since the program is not setuid and not normally called from remote programs, there may not be a typical attack vector for the issue that crosses privilege boundaries. Therefore this may not be a

vulnerability.

CVE-2004-2552 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF xboard-icshost-bo\(15362\)](#)

Secunia - Advisories - XBoard "-icshost"
Command Line Option Buffer Overflow
Vulnerability

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

[SECUNIA 11016](#)

[Exploit](#)
[Vendor Advisory](#)
[archives.neohapsis.com](#)
[text/x-c](#)
Inactive Link **Not Archived**

[FULLDISC 20040301 Smashing "XBoard 4.2.7\(All versions\)" For Fun & Profit.*Unpublished Local Stack Overflow Vulnerability!](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 4123](#)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tim Mann	Xboard	4.2.1	All	All	All
Application	Tim Mann	Xboard	4.2.2	All	All	All
Application	Tim Mann	Xboard	4.2.3	All	All	All
Application	Tim Mann	Xboard	4.2.4	All	All	All
Application	Tim Mann	Xboard	4.2.5	All	All	All
Application	Tim Mann	Xboard	4.2.6	All	All	All
Application	Tim Mann	Xboard	4.2.7	All	All	All
Application	Tim Mann	Xboard	4.2.1	All	All	All
Application	Tim Mann	Xboard	4.2.2	All	All	All
Application	Tim Mann	Xboard	4.2.3	All	All	All
Application	Tim Mann	Xboard	4.2.4	All	All	All
Application	Tim Mann	Xboard	4.2.5	All	All	All
Application	Tim Mann	Xboard	4.2.6	All	All	All
Application	Tim Mann	Xboard	4.2.7	All	All	All

```
cpe:2.3:a:tim_mann:xboard:4.2.1:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:tim_mann:xboard:4.2.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:tim_mann:xboard:4.2.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:tim_mann:xboard:4.2.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:tim_mann:xboard:4.2.5:*:*:*:*:*:
```

```
cpe:2.3:a:tim_mann:xboard:4.2.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:tim_mann:xboard:4.2.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:tim_mann:xboard:4.2.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:tim_mann:xboard:4.2.2:*:*:*:*:*:
```

```
cpe:2.3:a:tim_mann:xboard:4.2.3:*:*:*:*:*:*
```

cpe:2.3:a:tim_mann:xboard:4.2.4:*****:
cpe:2.3:a:tim_mann:xboard:4.2.5:*****:
cpe:2.3:a:tim_mann:xboard:4.2.6:*****:
cpe:2.3:a:tim_mann:xboard:4.2.7:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→