



# CVE-2004-2051

Published on: 07/24/2004 04:00:00 AM UTC

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

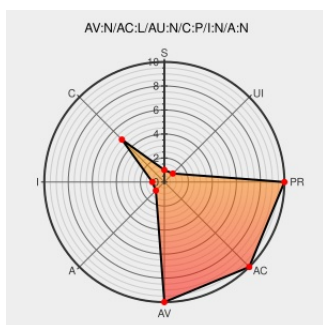
## CVE-2004-2051

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Thintune Extreme](#) from [Esesix](#) contain the following vulnerability:

The Phoenix browser in eSeSIX Thintune thin clients running firmware 2.4.38 and earlier allows local users to read arbitrary files via a file:/// URL.

CVE-2004-2051 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access  
Vector

**NETWORK**

Access  
Complexity

**LOW**

Authentication

**NONE**

Confidentiality  
Impact

**PARTIAL**

Integrity  
Impact

**NONE**

Availability  
Impact

**NONE**

## CVE References

Description

Tags

Link

No Description Provided

[www.osvdb.org](#)

[OSVDB 8249](#)

Inactive Link Not Archived

eSeSIX Thintune Thin Client Devices Multiple Vulnerabilities

[Exploit](#)  
[Vendor Advisory](#)  
[cve.report \(archive\)](#)  
[text/html](#)

[BID 10794](#)

Secunia - Advisories - Thintune Client Multiple Vulnerabilities

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

[SECUNIA 12154](#)

IBM X-Force Exchange

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

[XF thintune-url-obtain-information\(16798\)](#)

No Description Provided

[marc.info](#)  
[text/html](#)

[BUGTRAQ 20040724 eSeSIX Thintune thin client multiple vulnerabilities](#)

There are currently no QIDs associated with this CVE

| Type                                                                                                                                                                             | Vendor                 | Product                          | Version         | Update | Edition | Language |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|----------------------------------|-----------------|--------|---------|----------|
| Hardware       | <a href="#">Esesix</a> | <a href="#">Thintune Extreme</a> | 2.4.38_firmware | All    | All     | All      |
| Hardware       | <a href="#">Esesix</a> | <a href="#">Thintune Extreme</a> | 2.4.38_firmware | All    | All     | All      |
| Hardware       | <a href="#">Esesix</a> | <a href="#">Thintune L</a>       | 2.4.38_firmware | All    | All     | All      |
| Hardware       | <a href="#">Esesix</a> | <a href="#">Thintune L</a>       | 2.4.38_firmware | All    | All     | All      |
| Hardware       | <a href="#">Esesix</a> | <a href="#">Thintune M</a>       | 2.4.38_firmware | All    | All     | All      |
| Hardware   | <a href="#">Esesix</a> | <a href="#">Thintune M</a>       | 2.4.38_firmware | All    | All     | All      |
| Hardware   | <a href="#">Esesix</a> | <a href="#">Thintune Mobile</a>  | 2.4.38_firmware | All    | All     | All      |
| Hardware   | <a href="#">Esesix</a> | <a href="#">Thintune Mobile</a>  | 2.4.38_firmware | All    | All     | All      |
| Hardware   | <a href="#">Esesix</a> | <a href="#">Thintune S</a>       | 2.4.38_firmware | All    | All     | All      |
| Hardware   | <a href="#">Esesix</a> | <a href="#">Thintune S</a>       | 2.4.38_firmware | All    | All     | All      |
| Hardware   | <a href="#">Esesix</a> | <a href="#">Thintune Xm</a>      | 2.4.38_firmware | All    | All     | All      |
| Hardware   | <a href="#">Esesix</a> | <a href="#">Thintune Xm</a>      | 2.4.38_firmware | All    | All     | All      |
| Hardware   | <a href="#">Esesix</a> | <a href="#">Thintune Xs</a>      | 2.4.38_firmware | All    | All     | All      |
| Hardware   | <a href="#">Esesix</a> | <a href="#">Thintune Xs</a>      | 2.4.38_firmware | All    | All     | All      |

```
cpe:2.3:h:esesix:thintune mobile:2.4.38 firmware:*:*:*:*:*:*
```

|                                                     |
|-----------------------------------------------------|
| cpe:2.3:h:esesix:thintune_s:2.4.38_firmware:*****:  |
| cpe:2.3:h:esesix:thintune_s:2.4.38_firmware:*****:  |
| cpe:2.3:h:esesix:thintune_xm:2.4.38_firmware:*****: |
| cpe:2.3:h:esesix:thintune_xm:2.4.38_firmware:*****: |
| cpe:2.3:h:esesix:thintune_xs:2.4.38_firmware:*****: |
| cpe:2.3:h:esesix:thintune_xs:2.4.38_firmware:*****: |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)