



CVE-2009-0231

Published on: 07/15/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:29 PM UTC

CVE-2009-0231

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Windows 2000](#) from [Microsoft](#) contain the following vulnerability:

The Embedded OpenType (EOT) Font Engine (T2EMBED.DLL) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a crafted name table in a data record that triggers an integer truncation and a heap-based buffer overflow, aka "Embedded OpenType Font Heap Overflow Vulnerability."

CVE-2009-0231 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

US-CERT Technical Cyber Security Alert TA09-195A -- Microsoft Updates for Multiple Vulnerabilities

[US Government Resource](#)
www.us-cert.gov
[text/xml](#)

[CERT TA09-195A](#)

Public Advisory: 07.14.09 // iDefense Labs

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[IDEFENSE 20090714 Microsoft Embedded OpenType Font Engine \(T2EMBED.DLL\) Heap Buffer Overflow Vulnerability](#)

Microsoft Security Bulletin MS09-029 - Critical | Microsoft Docs

[docs.microsoft.com](#)
[text/html](#)

[MS MS09-029](#)

SecurityTracker.com Archives - Windows Embedded OpenType (FOT) Font Engine Buffer Overflow Lets Remote Users Execute

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

[SECTrack 1022543](#)

Arbitrary Code	text/html	
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:5457
No Description Provided	osvdb.org	 OSVDB 55842
	Inactive Link Not Archived	
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2009-1887
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
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x32	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x32	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	itanium	All
Operating System	Microsoft	Windows Server 2008	All	All	x32	All
Operating System	Microsoft	Windows Server 2008	All	All	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x32	All

System						
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Vista	All	All	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	-	sp1	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Vista	All	All	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	-	sp1	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	professional_x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp2	professional_x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
cpe:2.3:o:microsoft:windows_2000:*:sp4:*****:						
cpe:2.3:o:microsoft:windows_2000:*:sp4:*****:						
cpe:2.3:o:microsoft:windows_server_2003:*:sp2:*****:						
cpe:2.3:o:microsoft:windows_server_2003:*:sp2:*****:						
cpe:2.3:o:microsoft:windows_server_2008:*:*:itanium:*****:						
cpe:2.3:o:microsoft:windows_server_2008:*:*:x2:*****:						

CPG.E.O.O.IIIIGOSBUI.WHIIIGOWS_SGIVGI_2000. . .X02.

```
cpe:2.3:o:microsoft:windows_server_2008:*:*:x64:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x32:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x64:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows server 2008:-sp2:itanium:*.:.:.:
```

```
cpe:2.3:o:microsoft:windows server 2008:*:*:itanium:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2008:*:*:x32:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2008::*:x64:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x32:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows server 2008:*:sp2:x64:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2008:-sp2:itanium:*.:*:*.*.*
```

```
cpe:2.3:o:microsoft:windows_vista:*:*:x64:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_vista:*:sp2:x64:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_vista:-:sp1:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_vista:-:sp2:*.:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_vista:*:*:x64:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_vista:*:sp2:x64:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows vista:-sp1:*.:.:.:.:
```

```
cpe:2.3:o:microsoft:windows_vista:-:sp2:*.:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp2:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp2:professional_x64:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp2:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp2:professional_x64:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:*
```

No vendor comments have been submitted for this CVE

© [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](#)