

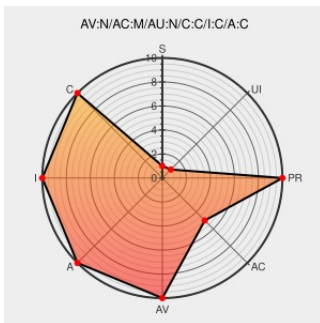


CVE-2015-6104

Published on: 11/11/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6104

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

Certain versions of [Windows 10](#) from [Microsoft](#) contain the following vulnerability:

The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Windows

Graphics Memory Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-6103.

CVE-2015-6104 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Issue 507 - google-security-research - Windows Kernel win32k.sys TTF font processing: pool-based buffer overflow with malformed TrueType program - Google Security Research - Google Project Hosting

[Exploit](#)
[Mailing List](#)
[Third Party Advisory](#)
[code.google.com](#)
[text/html](#)

code.google.com/p/google-security-research/issues/detail?id=507

Microsoft Windows Kernel Bugs Let Remote Users Execute Arbitrary Code and Local Users Bypass ASLR Restrictions and Gain Elevated Privileges - SecurityTracker

[Third Party Advisory](#)
[VDB Entry](#)
[www.securitytracker.com](#)
[text/html](#)

[SECTrack 1034114](#)

Microsoft Windows Kernel - 'win32k.sys' Malformed TrueType

[Exploit](#)

[EXPLOIT-DB 38713](#)

Program TTF Font Processing Pool-Based Buffer Overflow (MS15-115) - Windows dos Exploit

Third Party Advisory

VDB Entry

www.exploit-db.com

Proof of Concept

text/html

Microsoft Security Bulletin MS15-115 - Critical | Microsoft Docs

Patch

Vendor Advisory

docs.microsoft.com

text/html

 MS MS15-115

Microsoft Windows Kernel Win32k.sys TTF Font Processing Buffer Overflow ≈ Packet Storm

Third Party Advisory

VDB Entry

packetstormsecurity.com

text/html

 MISC
packetstormsecurity.com/files/134398/Microsoft-Windows-Kernel-Win32k.sys-TTF-Font-Processing-Buffer-Overflow.html

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 10	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt	-	All	All	All
Operating System	Microsoft	Windows Rt	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All

System						
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
cpe:2.3:o:microsoft:windows_10:-:*.*****:						
cpe:2.3:o:microsoft:windows_10:1511:*.*****:						
cpe:2.3:o:microsoft:windows_10:-:*.*****:						
cpe:2.3:o:microsoft:windows_10:1511:*.*****:						
cpe:2.3:o:microsoft:windows_7:-:sp1:*.*****:						
cpe:2.3:o:microsoft:windows_7:-:sp1:*.*****:						
cpe:2.3:o:microsoft:windows_8:-:*.*****:						
cpe:2.3:o:microsoft:windows_8:-:*.*****:						
cpe:2.3:o:microsoft:windows_8.1:-:*.*****:						
cpe:2.3:o:microsoft:windows_8.1:-:*.*****:						
cpe:2.3:o:microsoft:windows_rt:-:*.*****:						
cpe:2.3:o:microsoft:windows_rt:-:*.*****:						

cpe:2.3:o:microsoft:windows_rt_8.1:-:*:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_rt_8.1:-:*:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:itanium:*:
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64:*:
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:itanium:*:
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64:*:
cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:-:sp2:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_vista:-:sp2:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)