CVE-2011-3402

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2011-3402
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-11-04 21:55:04 UTC
Updated	2026-04-22 10:36:02 UTC
Description	Unspecified vulnerability in the TrueType font parsing engine in win32k.sys in the kernel-mode drivers in Microsoft Windows

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

EPSS: 0.895070000 probability, percentile 0.995570000 (date 2026-04-21)

CISA KEV: Listed on 2025-10-06; due 2025-10-27; ransomware use Unknown

Problem Types: NVD-CWE-noinfo | n/a | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9.3		AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Windows
Name	Microsoft Windows Remote Code Execution Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-087 ; https://nvd.nist.gov/vuln/detail/CVE-2011-3402

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All

Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Sc
US-CERT Alert TA12-164A -- Microsoft Updates for Multiple Vulnerabilities	af
The Day of the Golden Jackal – The Next Tale in the Stuxnet Files: Duqu Updated | Blog Central	af
Duqu: Status Updates Including Installer with Zero-Day Exploit Found | Symantec Connect Community	af
ISC Diary | Duqu Mitigation	af
Repository / Oval Repository	af
symantec.com has moved to broadcom.com	af
Microsoft Security Bulletin MS12-034 - Critical | Microsoft Docs	af
Repository / Oval Repository	af
www.cisa.gov/known-exploited-vulnerabilities-catalog	13
Security Alerts - Secunia	af
Microsoft Security Advisory (2639658): Vulnerability in TrueType Font Parsing Could Allow Elevation of Privilege	af
The Mystery of Duqu: Part Two - Securelist	af
Microsoft Security Bulletin MS11-087 - Critical | Microsoft Docs	af
404 - File Not Found | CISA	af
Security Alerts - Secunia	af
Windows OS Lets Remote Users Cause Arbitrary Code to Be Executed and Lets Local Users Gain Elevated Privileges - SecurityTracker	af
Microsoft releases Security Advisory 2639658 - MSRC - Site Home - TechNet Blogs	af
US-CERT Technical Cyber Security Alert TA11-347A -- Microsoft Updates for Multiple Vulnerabilities	af
US-CERT Alert TA12-129A - Microsoft Updates for Multiple Vulnerabilities	af
Repository / Oval Repository	af
Microsoft Security Bulletin MS12-039 - Important | Microsoft Docs	af
CVE Program record	CV
NVD vulnerability detail	NV
CISA Known Exploited Vulnerabilities catalog	CI

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2025-10-06T00:00:00.000Z	CVE-2011-3402 added to CISA KEV

There are currently no legacy QID mappings associated with this CVE.