CVE-2007-3030

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

Summary

CVE	CVE-2007-3030
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-07-10 22:30:00 UTC
Updated	2018-10-12 21:43:00 UTC
Description	Microsoft Excel 2000 SP3, 2002 SP3, 2003 SP2, and 2003 Viewer allows user-assisted remote attackers to execute arbitra

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Excel	2000	sp3	All	All
Application	Microsoft	Excel	2002	sp3	All	All
Application	Microsoft	Excel	2003	sp2	All	All
Application	Microsoft	Excel	2004	All	mac	All
Application	Microsoft	Excel	2007	All	All	All
Application	Microsoft	Excel	2000	sp3	All	All
Application	Microsoft	Excel	2002	sp3	All	All
Application	Microsoft	Excel	2003	sp2	All	All
Application	Microsoft	Excel	2004	All	mac	All
Application	Microsoft	Excel	2007	All	All	All
Application	Microsoft	Excel Viewer	2003	All	All	All
Application	Microsoft	Excel Viewer	2003	All	All	All

References

Reference
35959
[security bulletin] HPSBST02243 SSRT071446 rev.1 - Storage Management Appliance (SMA), Microsoft Patch Applicability MS07-036 to MS(

US-CERT Technical Cyber Security Alert TA07-191A -- Microsoft Updates for Multiple Vulnerabilities
Microsoft Excel Workspace Designation Remote Code Execution Vulnerability
SecurityTracker.com Archives - Microsoft Excel Caculation Error and Memory Corruption Error Lets Remote Users Execute Arbitrary Code
Microsoft Security Bulletin MS07-036 - Critical | Microsoft Docs
Microsoft Excel Multiple Code Execution Vulnerabilities - Advisories - Secunia
Repository / Oval Repository
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**