NVD - CVE-2017-0176

Archived: 2026-04-05 21:54:54 UTC

Description

A buffer overflow in Smart Card authentication code in gpkcsp.dll in Microsoft Windows XP through SP3 and Server 2003 through SP2 allows a remote attacker to execute arbitrary code on the target computer, provided that the computer is joined in a Windows domain and has Remote Desktop Protocol connectivity (or Terminal Services) enabled.

Metrics

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD

Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites 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 web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

URL	Source(s)	Tag(s)
http://www.securityfocus.com/bid/98550	CVE, Microsoft Corporation	Third Party Advisory VDB Entry

URL	Source(s)	Tag(s)
http://www.securityfocus.com/bid/98752	CVE, Microsoft Corporation	Third Party Advisory VDB Entry
https://blog.0patch.com/2017/06/a-quick-analysis-of-microsofts.html	CVE, Microsoft Corporation	
https://blog.fortinet.com/2017/05/11/deep-analysis-of-esteemaudit	CVE, Microsoft Corporation	Exploit Third Party Advisory
https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/	CVE, Microsoft Corporation	Patch Vendor Advisory
https://support.microsoft.com/en-us/help/4022747/security-update-for-windows-xp-and-windows-server-2003	CVE, Microsoft Corporation	Patch Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:o:microsoft:windows_server_2003:*:*:*:*:*:*:*:* Show Matching CPE(s)
cpe:2.3:o:microsoft:windows_server_2003:*:sp2:*:*:*:*:*:* Show Matching CPE(s)
cpe:2.3:o:microsoft:windows_xp:*:*:*:*:*:*:*:* Show Matching CPE(s)
cpe:2.3:o:microsoft:windows_xp:*:sp1:*:*:*:*:*:* Show Matching CPE(s)

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

Show Matching CPE(s)

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

Show Matching CPE(s)

Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

Change History

9 change records found show changes

Source: https://nvd.nist.gov/vuln/detail/CVE-2017-0176