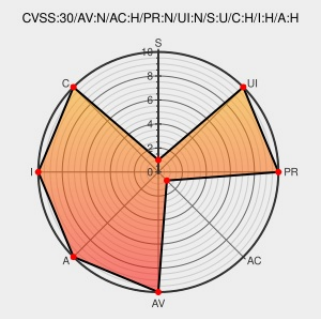
CVE-2016-3223

Published on: 06/15/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:02 PM UTC

CVE-2016-3223

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows 10 from Microsoft contain the following vulnerability:

Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandle LDAP authentication, which allows man-in-the-middle attackers to gain privileges by modifying group-policy update data within a domain-controller data stream, aka "Group Policy Elevation of Privilege Vulnerability."

CVE-2016-3223 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

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
Microsoft Windows 7 (x86/x64) - Group Policy Privilege Escalation (MS16-072) - Windows local Exploit	www.exploit-db.com Proof of Concept	EXPLOIT-DB 40219

	text/html	
Microsoft Windows 7 Group Policy Privilege Escalation ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/138248/Microsoft-Windows-7-Group-Policy-Privilege-Escalation.html
Microsoft Windows Unsafe Group Policy Update Lets Remote Users Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036100
Microsoft Security Bulletin MS16-072 - Important | Microsoft Docs	docs.microsoft.com text/html	MS MS16-072

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	All	sp1	All	All
Operating System	Microsoft	Windows 7	All	sp1	All	All
Operating System	Microsoft	Windows 8.1	All	All	All	All
Operating System	Microsoft	Windows 8.1	All	All	All	All
Operating System	Microsoft	Windows Rt 8.1	All	All	All	All
Operating System	Microsoft	Windows Rt 8.1	All	All	All	All
Operating System	Microsoft	Windows Server 2008	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All

System

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	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	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_8.1:*:*:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_8.1:*:*:*:*:*:*:*:*:
- 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:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_server_2008:*:sp2:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*:
- 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→