

[NT] Vulnerabilities in Kerberos Allow DoS, Information Disclosure, and Spoofing (MS05-042)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0039.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/10/05

To: list@securiteam.com

Date: 10 Aug 2005 14:57:01 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.secureteam.com/maillinglist.html>

Vulnerabilities in Kerberos Allow DoS, Information Disclosure, and Spoofing (MS05-042)

SUMMARY

A denial of service vulnerability exists that allows an attacker to send a specially crafted message to a Windows domain controller that could cause the service that is responsible for authenticating users in an Active Directory domain to stop responding. In addition an information disclosure and spoofing vulnerability allow an attacker to tamper with certain information that is sent from a domain controller and potentially access sensitive client network communication.

Users could believe they are accessing a trusted server when in reality they are accessing a malicious server. However, an attacker would first have to inject themselves into the middle of an authentication session between a client and a domain controller.

DETAILS

Affected Software:

* Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=4E34CD17-8710-4E22-8620-3B84139C18BB>>

Securiteam: [NT] Vulnerabilities in Kerberos Allow DoS, Information Disclosure, and Spoofing (MS05-042)

Download the update

- * Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=DD24F6FA-F6BB-4358-8C2F-7F6AB405981A>>

Download the update

- * Microsoft Windows XP Professional x64 Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=FB703DBD-3563-41FD-B608-361CC23796A5>>

Download the update

- * Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=34E7CF41-C584-4071-A36F-DE19D0D04B97>>

Download the update

- * Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=037CD6D6-11F7-4C44-9CFB-4B6D0B9B93CB>>

Download the update

- * Microsoft Windows Server 2003 x64 Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B86E688C-B668-4841-B961-7C5412C525EC>>

Download the update

Non-Affected Software:

- * Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

CVE Information:

Kerberos Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1981>>

CAN-2005-1981

PKINIT Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1982>>

CAN-2005-1982

Mitigating Factors for Kerberos Vulnerability – CAN-2005-1981:

- * An attacker must have valid logon credentials to exploit this vulnerability. The vulnerability could not be exploited by anonymous users.
- * This vulnerability only affects Windows 2000 Server and Windows Server 2003 domain controllers. Servers that do not perform the role of domain controllers are not affected.
- * Windows 2000 Professional and Windows XP are not affected by this vulnerability.
- * If an attacker successfully exploited this vulnerability, the affected system might display a warning that it would automatically restart after a 60-second countdown. At the end of this 60-second countdown, the affected system would automatically restart. After restart, the affected system would be restored to normal functionality. However, the affected system could be susceptible to another denial of service attack unless the update is applied.
- * Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are

connected to the Internet have a minimal number of ports exposed.

Workarounds for Kerberos Vulnerability – CAN-2005-1981:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

* Block UDP and TCP port 88 at the firewall

These ports are used to initiate a connection with Kerberos. Blocking them at the firewall will help prevent systems that are behind that firewall from attempts to exploit this vulnerability that originate outside the enterprise perimeter. We recommend that you block all unsolicited inbound communication from the Internet to help prevent attacks that may use other ports.

FAQ for Kerberos Vulnerability – CAN-2005-1981:

What is the scope of the vulnerability?

This is a denial of service vulnerability. An attacker who exploited this vulnerability could cause the server to automatically restart and, during that time, stop the server from responding to authentication requests.

This vulnerability exists in systems that perform the role of a domain controller, such as Windows 2000 Server or Window Server 2003. The only effect on clients is that they may not be able to log on to the domain if their domain controller stops responding.

What causes the vulnerability?

The method used by domain controllers to process specially crafted Kerberos messages.

What is Kerberos?

Windows 2000 and later operating system versions use Kerberos as the default authentication protocol. Kerberos provides secure user authentication. Also, because it is an industry standard, Kerberos permits interoperability." The Active Directory domain controller maintains user account and logon information to support the Kerberos service. For example, Kerberos is one protocol that is used to access data in Active Directory. For more information about Kerberos, visit the following

<<http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/security/kerberos.mspx>>

Kerberos Authentication Explained Web site or the

<<http://www.microsoft.com/technet/archive/security/news/kerb2000.mspx>> TechNet Web site.

What might an attacker use the vulnerability to do?

An attacker who exploited this vulnerability could cause the affected system to stop responding and the affected system to restart. The affected system might display a warning that it would automatically restart after a 60-second countdown. During this 60 second countdown, local authentication at the console of the affected system and user domain authentication with the affected system would not be possible. At the end of this 60-second countdown, the affected system would automatically restart. If users cannot perform domain authentication with the affected system, they might not be able to access domain resources. After restart, the affected system

would be restored to normal functionality. However, the affected system could be susceptible to another denial of service attack unless the update is applied. Even if a domain controller were completely unavailable, it would not prevent users who already had Kerberos tickets from using them. They could continue accessing all resources for which they had already been granted tickets. However, it would prevent the domain controller from issuing any new tickets to allow access to other resources.

Who could exploit the vulnerability?

Any authenticated user who could deliver the specially crafted Kerberos message to the affected system could try to exploit this vulnerability.

How could an attacker exploit the vulnerability?

An attacker could exploit this vulnerability by sending a specially crafted message to the domain controllers in a single forest or multiple forests, potentially causing a denial of service to domain authentication throughout an enterprise. This could cause the affected systems to stop responding and cause the affected systems to restart.

What systems are primarily at risk from the vulnerability?

Only Windows 2000 and Windows Server 2003 domain controllers are vulnerable.

I am running Windows 2000 Server or Windows Server 2003. What systems do I have to update?

The update to address this vulnerability must be installed on systems that are used as domain controllers. However, the update can be safely installed on servers in other roles. We recommend that you install this update on systems that might install Active Directory in the future.

Could the vulnerability be exploited over the Internet?

Yes. An attacker could try to exploit this vulnerability over the Internet. Firewall best practices and standard default firewall configurations can help protect against attacks that originate from the Internet. Microsoft has provided information about how you can help protect your PC. End users can visit the <http://go.microsoft.com/fwlink/?LinkId=21169> Protect Your PC Web site. IT professionals can visit the <http://go.microsoft.com/fwlink/?LinkId=21171> Security Guidance Center Web site.

What does the update do?

The update removes the vulnerability by modifying the way that Kerberos processes the specially crafted message.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

Mitigating Factors for PKINIT Vulnerability – CAN-2005-1982:

- * An attacker must have valid logon credentials and be able inject themselves into the middle of an authentication session between a client and a domain controller to exploit this vulnerability. The vulnerability could not be exploited by anonymous users.

- * An attacker can spoof an application server only to a target client for which the attacker has been granted permissions to access.

- * The account that is used by an attacker and the account that is used by the target of this attack would have to have their accounts enabled for smart card authentication. For more information about the required steps to enable smart card use within your enterprise, visit the following

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/b989f4fd-febd-42e1-a130-> Web site.

- * An attacker who successfully exploited this vulnerability could gain the same user rights as the target user.

Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

FAQ for PKINIT Vulnerability – CAN-2005-1982:

What is the scope of the vulnerability?

This is an information disclosure and spoofing vulnerability. This vulnerability could allow an attacker to tamper with certain information that is sent from a domain controller and potentially access sensitive client network communication. Users could believe they are accessing a trusted server when in reality they are accessing a malicious server. However, an attacker would first have to inject themselves into the middle of an authentication session between a client and a domain controller.

What causes the vulnerability?

The current implementation of the PKINIT protocol contains this issue as part of the design specification.

What is PKINIT?

PKINIT is an Internet Engineering Task Force (IETF) Internet Draft for "Public Key Cryptography for Initial Authentication in Kerberos." Windows 2000 and later uses draft 9 of the IETF "Public Key Cryptography for Initial Authentication in Kerberos" Internet Draft. Windows uses this protocol when you use a smart card for interactive logon. IETF Internet Drafts are available at the following <http://www.ietf.org/> IETF Web site.

What is Kerberos?

Windows 2000 and later operating system versions use Kerberos as the default authentication protocol. Kerberos provides secure user authentication. Also, because it is an industry standard, Kerberos permits interoperability." The Active Directory domain controller maintains user account and logon information to support the Kerberos service. For example, Kerberos is one protocol that is used to access data in Active Directory. For more information about Kerberos, visit the following <http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/security/kerberos.msp> Kerberos Authentication Explained Web site or the <http://www.microsoft.com/technet/archive/security/news/kerb2000.mspx> TechNet Web site.

What might an attacker use the vulnerability to do?

This vulnerability could allow an attacker to access sensitive information and spoof a domain controller. This could allow an attacker to view encrypted network communication that is sent between the client and the original destination.

Who could exploit the vulnerability?

An attacker must have valid logon credentials and be able inject themselves into the middle of an authentication session between a client and a domain controller to exploit this vulnerability. The vulnerability could not be exploited by anonymous users.

What systems are primarily at risk from the vulnerability?

Any domains where smart cards are actively in use could be at risk from this vulnerability.

What does the update do?

The update removes the vulnerability by modifying the way that PKINIT validates the data received.

Note In a domain environment, domain controllers and domain clients must install the security update to help protect against the PKINIT vulnerability.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been broadly publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued

ADDITIONAL INFORMATION

Securiteam: [NT] Vulnerabilities in Kerberos Allow DoS, Information Disclosure, and Spoofing (MS05-042)

The information has been provided by Microsoft Product Security.

The original article can be found at:

<http://www.microsoft.com/technet/security/Bulletin/MS05-042.mspx>

<http://www.microsoft.com/technet/security/Bulletin/MS05-042.mspx>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.