

[NT] Unchecked Buffer in PPTP Implementation Could Enable Denial of Service Attacks

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0137.html>

From: support@securiteam.com

Date: 10/31/02

From: support@securiteam.com

To: list@securiteam.com

Date: 31 Oct 2002 11:31:35 +0200

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

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Unchecked Buffer in PPTP Implementation Could Enable Denial of Service Attacks

SUMMARY

Windows 2000 and Windows XP natively support Point-to-Point Tunneling Protocol (PPTP), a Virtual Private Networking technology that is implemented as part of Remote Access Services (RAS). PPTP support is an optional component in Windows NT 4.0, Windows 98, Windows 98SE, and Windows ME.

A security vulnerability results in the Windows 2000 and Windows XP implementations because of an unchecked buffer in a section of code that processes the control data used to establish, maintain and tear down PPTP connections. By delivering especially malformed PPTP control data to an affected server, an attacker could corrupt kernel memory and cause the system to fail, disrupting any work in progress on the system.

The vulnerability could be exploited against any server that offers PPTP. If a workstation had been configured to operate as a RAS server offering PPTP services, it could likewise be attacked. Workstations acting as PPTP clients could only be attacked during active PPTP sessions. Normal operation on any attacked system could be restored by restarting the system.

DETAILS

Affected Software:

- * Microsoft Windows 2000
- * Microsoft Windows XP

Mitigating factors:

* As discussed in more detail in the FAQ, Microsoft has only successfully demonstrated denial of service attacks via this vulnerability. Because of how the overrun occurs, it does not appear that there is any reliable means of using it to gain control over a system.

* Servers would only be at risk from the vulnerability if they had been specifically configured to offer PPTP services. PPTP does not run by default on any Windows system. Likewise, although it is possible to configure a workstation to offer PPTP services, none operate in this capacity by default.

* Exploiting the vulnerability against a PPTP client could be difficult. PPTP is typically used in scenarios in which the client IP address changes frequently (e.g., because the client system is mobile). Not only would an attacker need to learn the IP address, but he or she would also need to mount an attack while the client had an active PPTP session underway.

Patch availability:

Download locations for this patch

* Microsoft Windows 2000:

<<http://www.microsoft.com/downloads/Release.asp?ReleaseID=43606>>
<http://www.microsoft.com/downloads/Release.asp?ReleaseID=43606>

* Microsoft Windows XP:

32-bit: <<http://www.microsoft.com/downloads/Release.asp?ReleaseID=43635>>
<http://www.microsoft.com/downloads/Release.asp?ReleaseID=43635>
64-bit: <<http://www.microsoft.com/downloads/Release.asp?ReleaseID=43631>>
<http://www.microsoft.com/downloads/Release.asp?ReleaseID=43631>

What's the scope of the vulnerability?

This is a denial of service vulnerability. An attacker who successfully exploited the vulnerability could potentially disrupt service on either clients or servers utilizing secure remote connections via the Point-to-Point Tunneling Protocol.

Exploiting the vulnerability against a client could be difficult, as it could only be exploited during an active remote networking session; in a typical usage scenario, the client would be a traveling system whose IP address would likely change frequently. Normal operation – for either client or server – could be restored by restarting the system.

What causes the vulnerability?

The vulnerability results because the code that implements the

Securiteam: [NT] Unchecked Buffer in PPTP Implementation Could Enable Denial of Service Attacks

Point-to-Point Tunneling Protocol in Windows 2000 and Windows XP contains an unchecked buffer in a section of code that processes PPTP control data.

What is Point-to-Point Tunneling Protocol?

Point-to-Point Tunneling Protocol (PPTP) is an industry standard protocol (defined in RFC 2637) that enables users to create and use virtual private networks (VPNs). Through VPN technologies such as PPTP, users can create secure connections to a remote network, even though the data may transit insecure networks like the Internet. (A good description of the technical underpinnings of PPTP is available from MSDN).

Windows 2000 and Windows XP include native support for PPTP. In server versions, PPTP support is implemented as an option within the Routing and Remote Access Service (RAS). In workstation versions, PPTP support is built into the Remote Access Client. PPTP support is an optional component in Windows NT 4.0, Windows 98, Windows 98SE, and Windows ME.

What's PPTP control data?

The data that constitutes a PPTP session can be categorized into two types – the data in the session, and the data about the session. Control data is the latter type of data. It's exchanged between the client and server to establish the session, make sure that it's still and active and healthy, and tear down the session when it's completed.

What's wrong with how the PPTP implementation handled control data?

The code that processes control data in the Windows 2000 and Windows XP implementations contains an unchecked buffer. By sending control data that had been malformed in a particular way, it could be possible to overflow the buffer and overwrite memory in the system kernel.

What could an attacker do via this vulnerability?

An attacker who successfully exploited this vulnerability could cause an affected system to fail. By targeting PPTP servers, the attacker could prevent users from being able to establish VPN sessions; by targeting PPTP clients, the attacker could cause them to fail with the loss of any work that was ongoing at the time. In either case, normal operation could be resumed by restarting the system.

Would it be possible to use this vulnerability to gain control over an affected system?

Frequently, buffer overruns can be used not only to disrupt a system's operation, but also to modify it in order to perform a task of the attacker's choosing and thereby gain control over the system. However, in this case, despite an extensive research effort, Microsoft has never been able to demonstrate any reliable way to gain control over a system. Instead, we have only been able to demonstrate a capability to exploit the vulnerability to disrupt system operation.

The reason has to do with the particular type of memory that would be overrun. In most buffer overruns, exploiting the vulnerability has the effect of putting the attacker's data into either of two data structures,

Securiteam: [NT] Unchecked Buffer in PPTP Implementation Could Enable Denial of Service Attacks

the stack or the heap. In such cases, the attacker can control to varying degrees where the data will reside and how it will be used. In this case, however, the data would overrun memory in the operating system kernel instead. Microsoft is unaware of any means of predicting where the data would spill, nor any way to use the data to modify system functionality.

Who could exploit the vulnerability?

Any user who could deliver data to a Windows 2000 or Windows XP system on which PPTP is running could exploit the vulnerability.

What's the risk to Windows servers?

A Windows 2000 server would only be at risk if the Routing and Remote Access (RRAS) service were running, and PPTP had been selected by the administrator as a supported protocol. In essence, this means that only servers that are specifically deployed to provide PPTP services would be at risk.

Windows NT 4.0 servers, even those providing PPTP services, are at no risk as the vulnerability does not affect the Windows NT 4.0 implementation of PPTP.

Would a firewall protect a server that offered PPTP services?

No. Recall that the purpose of PPTP is to provide secure communications across insecure media like the Internet. As a result, in order for a PPTP server to perform its designated role, the PPTP port (port 1723) on the firewall would need to be open.

What's the risk to Windows workstations?

There are two scenarios in which a Windows 2000 or Windows XP workstation could be at risk:

* If it had a PPTP session underway already. When a Windows client has an active outbound PPTP session, its PPTP service also listens for and will accept incoming control data on the PPTP port, and as a result the vulnerability could be exploited. It's worth noting, however, that the typical PPTP usage scenario could help mitigate these attacks. In contrast to servers, which usually occupy static, well-publicized IP addresses, workstations – especially traveling ones – tend to change their IP addresses frequently and therefore be more difficult to target.

* If it had been manually configured to operate as a RAS server. It is possible to manually configure a workstation to provide RAS services using PPTP and, if this had been done, the workstation would be at identical risk to a RAS server. It's worth noting that workstations are not frequently configured this way.

Workstations running any other version of Windows are at no risk from the vulnerability. Although a PPTP client is available for Windows 95, Windows 98, Windows 98SE and Windows ME, none of them include the vulnerability.

Securiteam: [NT] Unchecked Buffer in PPTP Implementation Could Enable Denial of Service Attacks

Would a firewall protect a PPTP client?

Yes. An active PPTP client that was protected by a firewall (including Internet Connection Firewall in Windows XP) or by a router that performs Network Address Translation (as most broadband routers do) would be protected from unsolicited messages directed to it at port 1723.

Do customers running Windows NT 4.0, Windows 98, Windows 98SE or Windows ME need to take any action?

No. The PPTP implementations in these versions do not contain the vulnerability.

What does the patch do?

The patch addresses the vulnerability by instituting proper buffer handling in the PPTP service.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:0_40078_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com>
Microsoft Product Security.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] Windows 2000 Default Permissions Could Allow Trojan Horse Program"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)