CERT Advisory CA-2003-04 MS-SQL Server Worm

Original release date: January 25, 2003
Last revised: January 27, 2003
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Microsoft SQL Server 2000
- Microsoft Desktop Engine (MSDE) 2000

Overview

The CERT/CC has received reports of self-propagating malicious code that exploits a vulnerability in the Resolution Service of Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000. This worm is being referred to as the SQLSlammer, W32.Slammer, and Sapphire worm. The propagation of this malicious code has caused varied levels of network degradation across the Internet and the compromise of vulnerable machines.

I. Description

The worm targeting SQL Server computers is self-propagating malicious code that exploits the vulnerability described in VU#484891 (CAN-2002-0649). This vulnerability allows for the execution of arbitrary code on the SQL Server computer due to a stack buffer overflow.

Once the worm compromises a machine, it will try to propagate itself. The worm will craft packets of 376-bytes and send them to randomly chosen IP addresses on port 1434/udp. If the packet is sent to a vulnerable machine, this victim machine will become infected and will also begin to propagate. Beyond the scanning activity for new hosts, the current variant of this worm has no other payload.

Activity of this worm is readily identifiable on a network by the presence of 376-byte UDP packets. These packets will appear to be originating from seemingly random IP addresses and destined for port 1434/udp.

II. Impact

Compromise by the worm confirms a system is vulnerable to allowing a remote attacker to execute arbitrary code as the local SYSTEM user. It may be possible for an attacker to subsequently leverage a local privilege escalation exploit in order to gain Administrator access to the victim system.

The high volume of 1434/udp traffic generated by hosts infected with the worm trying to find and compromise other SQL Server computers may itself lead to performance issues (including possible denial-of-service conditions) for Internet-connected hosts or for those computers on networks with compromised hosts.

III. Solution

Apply a patch

Administrators of all systems running Microsoft SQL Server 2000 and MSDE 2000 are encouraged to review CA-2002-22 and VU#484891. For detailed vendor recommendations regarding installing the patch see

http://www.microsoft.com/technet/security/virus/alerts/slammer.asp

SQL Server 2000 and MSDE 2000 both have the vulnerability documented in VU#484891. However, the propagation of the worm requires a process listening on port 1434/udp to exploit this vulnerability. This precondition is obviously present in SQL Server 2000. However, not all applications using MSDE 2000 listen to the network by default. Therefore, only certain MSDE 2000-enabled applications may be vulnerable.

Ingress/egress filtering

The following steps are only effective in limiting the damage that can be done by systems already infected with the worm. They provide no protection against the initial infection of systems. As a result, these steps are only recommended **in addition to** the preventative steps outlined above.

Ingress filtering manages the flow of traffic as it enters a network under your administrative control. Servers are typically the only machines that need to accept inbound traffic from the public Internet. In the network usage policy of many sites, external hosts are only permitted to initiate inbound traffic to machines that provide public services on specific ports. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound traffic to non-authorized services.

Egress filtering manages the flow of traffic as it leaves a network under your administrative control. There is typically limited need for machines providing public services to initiate outbound connections to the Internet.

In the case of this worm, employing ingress and egress filtering can help prevent compromised systems on your network from attacking systems elsewhere. Blocking UDP datagrams with both source or destination ports 1434 from entering or leaving your network reduces the risk of external infected systems communicating with infected hosts inside your network.

Recovering from a system compromise

If you believe a system under your administrative control has been compromised, please follow the steps outlined in

> Steps for Recovering from a UNIX or NT System Compromise

Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are compromised, please send mail to cert@cert.org with the following text included in the subject line: "[CERT#35663]".

Feedback can be directed to the author: Roman Danyliw

This document is available from: http://www.cert.org/advisories/CA-2003-04.html

---

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

> http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

> http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

January 25, 2003: Initial release
January 26, 2003: Updated VU# information, packet size, MS Advisory link
January 27, 2003: MSDE 2000
October 25, 2021: fixed typo in Impact "compromised hosts"