QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ May 03, 2004

Sasser Worm

ADVISORY OVERVIEW

May 03, 2004 – Qualys™ Vulnerability R&D Labs has released a new vulnerability signature in the QualysGuard® Web Service to protect organizations against the new Sasser Worm and related variants. Customers can immediately audit their networks for the worm and the vulnerability being exploited by accessing their QualysGuard subscription. The vulnerability that Sasser exploits was added to the QualysGuard audit database April 13, 2004 (QID 90108).

WORM DETAILS

The Sasser worm (W32.Sasser.A and its variants) is currently circulating on the Internet. The Sasser worm exploits the Local Security Authority Subsystem Service (LSASS) issue that was addressed by the security update released on April 13 in conjunction with Microsoft Security Bulletin MS04-011. The Sasser worm spreads by scanning randomly chosen IP addresses on TCP port 445 and exploiting the LSASS vulnerability.

HOW TO IDENTIFY IF SYSTEMS HAVE BEEN INFECTED

Audits for the Sasser worm and its variants are already available in the QualysGuard vulnerability management platform. A default scan will detect these issues and is the recommended detection method. In addition QualysGuard users can perform a selective scan for these specific vulnerabilities using the following checks:

- “Sasser Worm Detected (Versions A to C)”
    - Qualys ID: 1135
    - Limit the scan to TCP ports 139, 445 and 5554
    - A Windows login is not required, but using one will provide an added level of detection.
    - Additionally, enable the “Windows Host Name” signature with Qualys ID 82044 if you want to report on vulnerable hosts by Windows (NetBIOS) machine name.

HOW TO IDENTIFY VULNERABLE SYSTEMS

Audits for the Microsoft April 2004 Security Bulletin vulnerabilities were available in the QualysGuard vulnerability management platform on April 13, 2004. A default scan will detect these issues and is the recommended detection method. In addition QualysGuard users can perform a selective scan for these specific vulnerabilities using the following checks:

- "Multiple Microsoft Windows Vulnerabilities (MS04-011)"
  - Qualys ID: 90108
  - Limit the scan to TCP ports 25, 80, 135, 139, 443, 445 and 593
  - A Windows login is not required, but using one will provide an added level of detection.
  - Additionally, enable the "Windows Host Name" signature with Qualys ID 82044 if you want to report on vulnerable hosts by Windows (NetBIOS) machine name.

TECHNICAL SUPPORT

For more information, customers can contact Qualys Technical Support directly at support@qualys.com or 1-866-801-6161.

Complete information about using QualysGuard's Windows Authentication feature is available in the on-line help. To access the information click Help, Network Analysis (Scans) then Windows Authentication.

ABOUT QUALYSGUARD

QualysGuard is an on-demand security audit service delivered over the web that enables organizations to effectively manage their vulnerabilities and maintain control over their network security with centralized reports, verified remedies, and full remediation workflow capabilities with trouble tickets. QualysGuard provides comprehensive reports on vulnerabilities including severity levels, time to fix estimates and impact on business, plus trend analysis on security issues. By continuously and proactively monitoring all network access points, QualysGuard dramatically reduces security managers' time researching, scanning and fixing network exposures and enables companies to eliminate network vulnerabilities before they can be exploited.

Access for QualysGuard customers: https://qualysguard.qualys.com

Free trial of QualysGuard service: http://www.qualys.com/forms/maintrial.html