Nmap Potential Insecure File Creation Vulnerability

Synopsis

Bugtraq ID	10567	CVE	CVE-MAP-NOMATCH
Published	Jun 18 2004		
Classification	Race Condition Error		
Remote	No	Local	Yes
Availability	Circumstantial	Authentication	Not Required
Ease	No Exploit Required		
Last Update	6/18/2004 4:49:35 PM GMT		
Last Change	This BID is being retired.		

Urgency Rating 5.4

Threat Breakdown

Severity	4.4
Impact	6
Ease of Exploit	1
Credibility	Single Source

Vulnerable Systems

Fyodor nmap 2.53.0
Fyodor nmap 3.45.0
Fyodor nmap 3.45.0 -1
Fyodor nmap 3.46.0
Fyodor nmap 3.47.0
Fyodor nmap 3.48.0
Fyodor nmap 3.48.0 -1
Fyodor nmap 3.50.0
Fyodor nmap 3.50.0 -1
Fyodor nmap 3.51.0

Short Summary

Nmap is reported prone to a potential insecure file creation vulnerability.

Impact

Local attackers may corrupt files in the context of the user invoking the application. This will likely result in destruction of data or a denial of service but could also potentially be exploited to elevate privileges.

Technical Description

Nmap is an open source port scanning utility. It is available for UNIX, Linux, and Microsoft platforms.

Nmap is reportedly prone to a potential insecure file creation vulnerability. A local user may exploit this vulnerability to cause files to be overwritten with the privileges of the user running Nmap.

It is reported that when Nmap is launched with the '-oN' option, the application stores the results in a log file specified by the user. The presence of this file is not verified by the application. In the instance that the attacker has sufficient write access, they could exploit this issue by creating a symbolic link that is named after the log file. When the program is run, the file pointed to by the symbolic link may be corrupted, if it is writeable by the user invoking the program.

Reportedly, the exploitation of this issue is circumstantial and may only be exploited when Nmap does not recognize a service during a scan. The data returned and logged by the application can be influenced to gain elevated privileges.

All versions of Nmap are considered to be vulnerable to this issue.

Further analysis has showed that this issue is not a vulnerability. This BID is being retired.

Attack Scenarios

The attacker must have local access to the system to exploit this issue. For successful exploitation to occur, the attacker must also be able to create a symbolic link in a directory of the user who is expected to run the application. The application must also be run with the '-oN' command line option to enable logging to a hard-coded log file. The Nmap scan must also result in the application not recognizing a targeted service.

If the conditions are met, the attacker will exploit the issue by creating a symbolic link that points to a system file that is writeable by the user who is expected to run the program. When the program is run, it will perform operations on the file pointed to by the symbolic link instead of the legitimate log file.

This will most likely result in destruction of files, possibly causing a denial of service. There is also a potential for privilege escalation.

Exploits

The following proof of concept is available:

http://www.infohacking.com/INFOHACKING_RESEARCH/Our_Advisories/nmap/server.sh

Mitigating Strategies

Permit local access for trusted individuals only. Where possible, use restricted environments and restricted shells.

Do not permit untrusted individuals to have local interactive access to a vulnerable computer.

Run all software as a non-privileged user with minimal access rights.

All non-administrative tasks should be performed as an unprivileged user with minimal access rights. This will reduce the impact of latent vulnerabilities in various applications.

Solutions

Currently we are not aware of any vendor-supplied patches for this issue. If you feel we are in error or are aware of more recent information, please mail us at: vuldb@securityfocus.com <mailto:vuldb@securityfocus.com>.

Credit

Discovery is credited to Hugo "Vázquez" "Caramés" <hugo@infohacking.com>.

References

Web Page:Nmap Home Page (Fyodor) Fyodor

http://www.insecure.org/nmap/

Change Log

2004.06.18: This BID is being retired.
2004.06.18: Initial analysis.

URL

https://alerts.symantec.com/members/display_alert.asp?AlertType=1&id=10567