

Samba SMBD Remote Denial of Service Vulnerability

iDEFENSE Security Advisory 11.08.04:

I. BACKGROUND

Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients.

II. DESCRIPTION

Remote exploitation of an input validation error in Samba could allow an attacker to consume system resources and potentially cause the target system to crash.

The problem specifically exists within the `ms_fnmatch()` routine which upon parsing '*' characters within a pattern will fall into an exponentially growing loop. The responsible section of vulnerable code appears here:

```
case '*':
    for (; *n; n++) {
        if (ms_fnmatch(p, n) == 0) return 0;
    }
    break;
```

An authenticated remote attacker can cause a resource exhaustion attack by sending multiple malformed commands to an affected server. A request as simple as `'dir *****z'` can trigger this condition leading to 100% CPU usage.

III. ANALYSIS

Successful exploitation allows authenticated remote attackers to exhaust CPU resources. This attack takes very little bandwidth and can, in some cases, cause the machine to stop responding. Multiple attacks can be launched in parallel which can make this attack more effective.

IV. DETECTION

iDEFENSE has confirmed the existence of this vulnerability in Samba versions 3.0.4 and 3.0.7. It is suspected that all versions of Samba up to and including 3.0.7 are vulnerable.

V. WORKAROUND

Restricting access to the server by using the "hosts allow" setting in `smb.conf` and/or applying firewall rules may help mitigate this vulnerability.

VI. VENDOR RESPONSE

3.0.7 patch:

<http://www.samba.org/samba/ftp/patches/security/samba-3.0.7-CAN-2004-0930.patch>

3.0.7 patch signature:

<http://www.samba.org/samba/ftp/patches/security/samba-3.0.7-CAN-2004-0930.patch.asc>

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the names CAN-2004-0930 to these issues. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.