Technical Support Bulletin

Samba Security Issues Affect EXAScaler NFS/SMB Data Services

ALERT! Samba security vulnerabilities in EXAScaler NFS/SMB Data Services enable malicious attackers to break network authentication, inject code in long DCE/RPC messages, or take over root privileges.

Issue Summary

Three notable security vulnerabilities in Samba affect EXAScaler NFS/SMB Data Services. These are:

- CVE-2016-2124 **Moderate.** SMB1 client connections can be downgraded to plaintext authentication or Windows Challenge/Response (NTLM) authentication using a man-in-the-middle attack, even if Kerberos authentication is requested. *(Samba bug #12444)*
- CVE-2021-23192 **Moderate.** A flaw in packet verification permits large DCE/RPC messages, when broken into multiple packets over an insecure transport channel, to be intercepted and alternate packet contents substituted, potentially changing server behavior. *(Samba bug #14875)*
- CVE-2020-25717 **Important.** Root takeover can be forced from Active Directory when a Kerberos Privileged Attribute Certificate (PAC) is not required. *(Samba bug #14556)*

Affected Products

EXAScaler NFS/SMB Data Services versions 5.2.4 and lower, as well as 6.0.0 in the 6.x.x series, are affected by these issues.

Resolution

These issues will be resolved in future releases of NFS/SMB Data Services.

Workarounds

Until a full resolution becomes available, customers are advised to apply the following workarounds.

CVE-2016-2124 - SMB1 CLIENT CONNECTIONS DOWNGRADED TO PLAINTEXT AUTHENTICATION

The default configuration for NFS/SMB Data Services is not vulnerable to this issue. However, customized configuration settings may expose your system to risk. This issue is possible only when the following Samba parameters are set concurrently:

```
client NTLMv2 auth = no
client lanman auth = yes
client plaintext auth = yes
client min protocol = NT1 # or lower
```

However, NFS/SMB Data Services does default to a problematic value for the `client min protocol` parameter. DDN Engineering recommends customers disable SMB1 and earlier protocols with the following command:

```
docker exec nsds net conf setparm global "client min protocol" SMB2_02
```

CVE-2021-23192 - PACKET VERIFICATION ISSUE WITH LARGE DCE/RPC MESSAGES

This issue can be prevented with the following command:

```
docker exec nsds net conf setparm global "dcesrv:max auth states" 0
```

CVE-2020-25717 - ROOT TAKEOVER FROM ACTIVE DIRECTORY

This issue occurs when a DOMAIN\user lookup fails. If `nss_winbind` is in use for authentication, you can prevent such lookup failures by ensuring that Kerberos PACs are required. Enter the following parameter in the `smb.conf` file:

```
gensec:require_pac=true
```

Active Directory administrators can further prevent exploitation of this issue by creating disabled user accounts for privileged Linux/Unix user names in Active Directory domains, particularly `root`, `ubuntu`, and all users under 1000 in `/etc/passwd`. Also protect `admin` for web applications. For example:

```
samba-tool user add root -H ldap://$SERVER -U$USERNAME%$PASSWORD --random-password
samba-tool user add ubuntu -H ldap://$SERVER -U$USERNAME%$PASSWORD --random-password
```

ALERT! An audit may be required to ensure that malicious accounts corresponding to Linux/Unix system accounts are not already in place in Active Directory domains.

Administrators should also consider setting `ms-DS-MachineAccountQuota` to 0 in Active Directory domains if this capability is not being used.

Contacting DDN Technical Support

Please contact DDN Technical Support at any time if you have questions or need assistance. Support can be reached by phone, by email, or on the web as listed below.

Web

DDN Community Support Portal	https://community.ddn.com/login
Portal Assistance	webportal.support@ddn.com

Email

Support Email	support@ddn.com

Telephone

DDN Support Worldwide Directory	https://www.ddn.com/support/global-services-overview/

Bulletins & Notices

Support Bulletins	http://www.ddn.com/support/technical-support-bulletins
End-of-Life Notices	http://www.ddn.com/support/end-of-life-notices
Release Notes	https://community.ddn.com/login
TSB Subscription Requests	support-tsb@ddn.com