DDN® STORAGE

TECHNICAL SUPPORT BULLETIN

DDN TECHNICAL SUPPORT | SPT-TSB-0063 (A2) | 12 DECEMBER 2016

CVE-2016-5195

"Dirty COW" Copy-on-Write Security Vulnerability in Linux Kernel

Privilege Escalation Exploit

Red Hat Product Security has been made aware of an important privilege escalation security vulnerability in the Linux kernel. This vulnerability, known in the trade press as "Dirty COW", has been assigned CVE-2016-5195 in the Common Vulnerabilities and Exposures (CVE®) database. This vulnerability affects most modern Linux distributions, and therefore affects DDN storage products.

The Dirty COW vulnerability takes advantage of a race condition in the way the Linux kernel's memory subsystem handles the copy-on-write (COW) breakage of private read-only memory mappings. An attacker with a local system account could use this flaw to gain write access to otherwise read-only memory mappings and then increase their privileges on the system.

An exploit using this technique has been found "in the wild." Exploitation requires local access to the system. It does not leave any trace of anything abnormal happening in the logs.

A video explanation of the exploit is available online here.

Affected Systems

The Dirty COW issue has existed since kernel version 2.6.22, which was released in 2007. This issue affects Linux kernel packages shipped with Red Hat Enterprise Linux 5, 6, 7 and MRG 2.x, as well as equivalent CentOS 5, 6 and 7 releases. The vulnerability also affects Debian, SuSE & Ubuntu Linux distributions. A fix was posted on Git in October 2016.

Affected DDN Products

The table below lists currently supported DDN products affected by the Dirty COW issue. DDN's plans for addressing the issue are summarized here per DDN's Security Policy.

DDN PRODUCT	AFFECTED VERSIONS	FIX	FIX AVAILABILITY
Storage Arrays			
IME *(IME14K or software)*	1.0	1.1	Q1 2017
SFA OS *(SFA14K, SFA12K, SFA7700)*	3.0.1.5 and earlier 2.3.1 and earlier	3.1.0.1	***Now***
SFA OS *(SFA10K)*	2.2.7 and earlier	Future release	Q1 2017
SFA OS *(S2A6620)*	1.5.7 and earlier	Not planned	—
WOS Core *(WOS6000, WOS7000, WOS9660, software)*	2.7.0 and earlier	2.7.1	Q1 2017
Storage Solutions			
DirectMon	2.5.0 and earlier	Future release	To be determined
EXAScaler	2.4.0 and earlier 2.3.1 and earlier	3.0.0 2.4.1	Q4 2016 Q1 2017
EXAScaler Bridge	1.0	1.0.1	Q4 2016
GRIDScaler *(RHEL, CentOS)*	4.0.0 and earlier 3.2.2 and earlier	4.1.0 3.2.3	***Now*** Q1 2017
GRIDScaler *(OEL)*	3.2.2 and earlier	3.2.3	Q1 2017
GRIDScaler Bridge	1.8.0 and earlier	1.8.1	***Now***
WOS Access CIFS/SMB/NFS	1.5.0 and earlier	1.6.1	***Now***
WOS Access S3/Swift	2.2.1 and earlier	2.3.0	Q2 2017

Determining Vulnerability in Non-DDN Linux Distributions

Customers running a DDN solution under their own installation of Linux rather than a DDN-provided Linux distribution may be vulnerable to the Dirty COW exploit separately from their DDN product. For these customers, Red Hat has provided a detection script that can be run locally with Bash to determine whether a system is affected by Dirty COW. You can download that script here.

Customers running their own installation of Red Hat Enterprise Linux (RHEL) may also refer to following table to determine whether their system could be vulnerable to the Dirty COW exploit. The table lists RHEL kernel versions containing the fix. ***Kernel versions prior those listed are vulnerable***.

RELEASE	KERNEL VERSION WITH FIX
RHEL 7.1 EUS	3.10.0-229.42.2.el7
RHEL 7	3.10.0-327.36.3.el7
RHEL 6	2.6.32-642.6.2.el6
RHEL 6 EUS	2.6.32-573.35.2.el6
RHEL 6 AUS	2.6.32-431.75.1.el6
RHEL 5	2.6.18-416.el5

Resolution

To eliminate the possibility of a Dirty COW exploit, do the following:

- Upgrade your DDN product to the fix release as soon as it becomes available.
- If you run a DDN solution under your own Linux installation, update the Linux kernel packages on your system using the packages released with the errata listed below. (Remember to reboot the system after updating.) A full listing of advisories and updates is available from Red Hat here.

LINUX RELEASE	ERRATA
RHEL Server 7.1 EUS	https://rhn.redhat.com/errata/RHSA-2016-2118.html
RHEL Server 7	https://rhn.redhat.com/errata/RHSA-2016-2098.html
RHEL Server 6.7 EUS	http://rhn.redhat.com/errata/RHSA-2016-2106.html
RHEL Server 6.5 AUS	https://rhn.redhat.com/errata/RHSA-2016-2120.html
RHEL Server 6	http://rhn.redhat.com/errata/RHSA-2016-2105.html
RHEL 5	https://rhn.redhat.com/errata/RHSA-2016-2124.html
CentOS 7	https://lists.centos.org/pipermail/centos-announce/2016-October/022133.html
CentOS 6	https://lists.centos.org/pipermail/centos-announce/2016-October/022134.html
CentOS 5	https://lists.centos.org/pipermail/centos-announce/2016-October/022135.html

Contacting DDN Technical Support

Please contact DDN Technical Support at any time if you have questions or require 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

Telephone

DDN Support Worldwide Directory	http://www.ddn.com/support/contact-support

Email

Support Email	support@ddn.com

Bulletins

Support Bulletins	http://www.ddn.com/support/technical-support-bulletins
End-of-Life Notices	http://www.ddn.com/support/end-of-life-notices
Bulletin Subscription Requests	support-tsb@ddn.com