SECURITY ADVISORY – “Dirty COW” Linux Kernel Vulnerability (CVE-2016-5195)
Advisory Version 1.1

Security Advisory Relating to “Dirty COW” Vulnerability on Various Polycom Products.

DATE PUBLISHED: November 3, 2016

Polycom is conducting ongoing research to determine the level of vulnerability (if any) for each of its various products.

Any information in this advisory is subject to change and additional information will be added as it becomes available.

Please Note: This is a living document, updated regularly until any product affected by any of the vulnerabilities in this advisory has been repaired against that vulnerability. The newest version of this document will always reside at the following URL:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

Vulnerability Summary

A high-severity vulnerability has been recently disclosed in most modern versions of the Linux kernel. This vulnerability could allow an attacker with non-root shell access to elevate their privileges to that of a root user. The vulnerability is known as “Dirty COW” and has been assigned the following CVE identifier: CVE-2016-5195:

https://www.theguardian.com/technology/2016/oct/21/dirty-cow-linux-vulnerability-found-after-nine-years

Details

CVE-2016-5195, aka “Dirty COW”

Dirty COW attack against the Linux kernel – Dirty COW allows an attacker to exploit a race condition in the Linux kernel’s memory subsystem. This allows an unprivileged shell user to gain write access to otherwise read-only memory which in turn allows the attacker to potentially gain root privileges and control the system.

Mitigations

Polycom recommends that customers disable telnet/ssh shell access for all products.

Furthermore, Polycom recommends that customer evaluate network access control lists, firewalls and other network protections to ensure that they have been deployed in a manner that is consistent with security best practices.

The risk presented by this potential vulnerability to Polycom products, as well as other networked devices, may be mitigated by these controls. Customers should also ensure that Polycom products have been configured as recommended by Polycom implementation guides. Customers may wish to implement additional event monitoring and review until such time that an update is installed.

Products Affected

Note that the products listed in the below table are the only products whose vulnerability status can be definitively stated at this time – to the positive or the negative. Any products not listed in this chart remain under investigation, and will appear in this chart as soon as their status is known.

Media Manager – All versions	Not vulnerable
CX5000 – All versions	Not vulnerable
CX Product Line – All versions	Not vulnerable
RealPresence Mobile – All versions	Not vulnerable
RealPresence Desktop – All versions	Not vulnerable
RealPresence Group Series – All versions	No shell available to non-privileged users to exploit Dirty Cow
RealPresence Touch – All versions	No shell available to non-privileged users to exploit Dirty Cow
Polycom Touch Control – All versions	No shell available to non-privileged users to exploit Dirty Cow
HDX – All versions	No shell available to non-privileged users to exploit Dirty Cow
Video Border Proxy (VBP) – All versions	No shell available to non-privileged users to exploit Dirty Cow
ISDN Gateway – All versions	No shell available to non-privileged users to exploit Dirty Cow
Polycom Phones (VVX, SPIP, SSIP, Trio) – All versions	No shell available to non-privileged users to exploit Dirty Cow
RealPresence Debut – All versions	No shell available to non-privileged users to exploit Dirty Cow
RealPresence MediaSuite – All versions	No shell available to non-privileged users to exploit Dirty Cow

RealAccess – All versions	No shell available to non-privileged users to exploit Dirty Cow
Video Border Proxy (VBP) – All versions	No shell available to non-privileged users to exploit Dirty Cow
RealPresence Resource Manager – All versions	No shell available to non-privileged users to exploit Dirty Cow
RealPresence DMA – All versions	No shell available to non-privileged users to exploit Dirty Cow
RealPresence Access Director – All versions	No shell available to non-privileged users to exploit Dirty Cow

CVSS Base Metrics:

To assist our customers in the evaluation of this vulnerability, Polycom leverages the Common Vulnerability Scoring System (CVSS). This system provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities that better enable our customers to make informed decisions and assess the impact on their environment.

Base CVSS v2 Score: 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)

Base CVSS v3 Score: 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

For more information on CVSS v2 and v3 please see:
https://www.first.org/cvss/v2/guide
https://www.first.org/cvss/specification-document

Severity: Critical

Rating	Definition
Critical	A vulnerability, which, if exploited would allow malicious code to execute, potentially without a user being aware.
High	A vulnerability, which, if exploited could impact the confidentiality, integrity, or availability of data, or of the integrity or availability of resources.
Medium	A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.
Low	A vulnerability that has minimal impact to the system and is extremely difficult to exploit.

Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment should contact Polycom Technical Support – either call 1-800-POLYCOM or visit:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

For the latest information. You might also find value in the high-level security guidance and security news located at:

http://www.polycom.com/security

Revision History

Revision 1.0 - Original publication: October 26, 2016
Revision 1.1 - Original publication: November 3, 2016