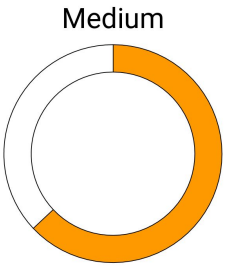
SMC IPMI Virtual Hardware Vulnerability - USBAnywhere September 2019



Advisory ID	nutanix-sa-016-virtmedia	CVE(s)
		None Provided by SMC
Last Updated	18 December 2019	
Published	04 September 2019	
Version	9	

Final Update

Summary

On Tuesday, September 3rd 2019, SuperMicro (SMC) disclosed a medium severity vulnerability in their Baseboard Management Controller (BMC) firmware for their X9, X10 and X11 based server products. This disclosure was the same vulnerability reported by multiple media outlets of the findings by security researchers at Eclypsium around a virtual media vulnerability within certain Supermicro (SMC) Baseboard Management Controller (BMC) versions. Dubbed USBAnywhere, this vulnerability takes advantage of weak or non-existent encryption during authentication with the virtual media service running on tcp and udp port 623 within the BMC.

Information on Vulnerabilities

CVE IDs and their corresponding CVSS scores are not currently available from SMC.

Leveraging this vulnerability relies on a few factors. Note that knowledge of authentication credentials is unnecessary so long as a valid account has accessed the service since it was last powered on. This is due to a lingering state issue within the BMC for the Virtual Media service that allows for authentication bypass if a client happens to connect with the same socket file descriptor and information as a previously valid client.

Additionally, due to the way the BMC handles USB descriptors it is possible to mount USB devices that can not only exfiltrate data, but also inject keystrokes into the host operating system. The combination of these factors leaves a malicious actor in a position to exploit the host operating system in a number of ways.

Tel: 1 (855) 688-2649 | Fax: 1 (408) 916-4039 | Email: security@nutanix.com

Affected Products

This document will be updated with the patch release schedules. Please check the Nutanix Support Portal - Security Advisories for the latest update.

Nutanix Products

Product	Fix Release
All NX Hardware Platforms (G3 - G7)	*X11 (G6 / G7) BMC Version 7.05* *X10 (G4 / G5) BMC Version 3.64* *LCM version 2.3 has shipped with the above updated BMC Firmware in version 2.3.* *Note: For compatibility with the above BMC Firmware updates, Foundation 4.4.4 or greater will be required.*

Mitigations

Risk can be mitigated immediately for this vulnerability while a fix is being worked on by SMC.

The key vector of this vulnerability is the authentication path between software and the Virtual Media service running on tcp and udp port 623 of the BMC. During this handshake, authentication credentials are sent in the clear (unencrypted) and data passed over that port post-authentication is unencrypted.

Risk can be managed via the following methods until a patch is released.

- Architecture - Baseboard Management Controllers, IPMI and other server management interfaces are not to be placed on untrusted networks, especially not internet facing networks. Proper and accepted architecture and best practice is to place these interfaces on isolated and protected areas of the network. If IPMI and BMC access is required within your data center ensure that those devices are on a trusted network with appropriate network access controls in place.

- Availability - If IPMI and BMC access is *not* critical within your data center, you can temporarily disable it via KB 8114. Note that disabling port 623 will completely mitigate the attack vector; however, it will affect the following Nutanix functionality.

    - Bare-Metal Foundation (Used during installation / expansion. Note: New node from the factory will not be impacted. However, one needs to disable tcp/udp 623 port after adding node to cluster)
    - Host Boot Drive Replacement (SATADOM for G3, G4 and G5 / M.2 for G6)

Tel: 1 (855) 688-2649 | Fax: 1 (408) 916-4039 | Email: security@nutanix.com

- Stand-Alone Foundation - Expand Node

Sources

Supermicro Security Information - https://www.supermicro.com/support/security_BMC_virtual_media.cfm
Eclypsium - https://eclypsium.com/2019/09/03/usbanywhere-bmc-vulnerability-opens-servers-to-remote-attack/
Nutanix KB Article - https://portal.nutanix.com/kb/8114

Support

If you have questions, please open a case with Nutanix Support at http://portal.nutanix.com, or by calling Support at the phone number on the website http://www.nutanix.com/support.

Thank you for being a Nutanix customer.

Revision History

Version	Section	Date
1	-	04 September 2019
2	Updated release information and dates	11 September 2019
3	Information validated	18 September 2019
4	Releases vehicles and timelines	03 October 2019
5	Version number change	17 October 2019
6	Updated release	04 November 2019
7	Updated release	20 November 2019
8	Updated timelines	05 December 2019
9	Removal of items and closure	18 December 2019