Firmware Fixes to Common Vulnerabilities and Exposures

Supermicro pro-actively works with security community to identify and strengthen security across our product line. Please find solutions to CVEs published on Supermicro firmware.

For other resolved security issues, please refer to release notes of each product.

Document Last Update: 7/27/2015

BMC Firmware Security Fixes:

SMT X10 2.13, SMT X9 and X8 (Custom Firmware)
GHOST: glibc vulnerability (CVE-2015-0235)

SMT X10 176, SMT X9 335, SMM X9 259, SMT X8 320,
POODLE SSLv3 (CVE-2014-3566)

SMT X9 319, SMT_X8_320
Weak hash for RAKP (CVE-2013-4786)

SMT X9 317, SMT X8 312
Static Encryption Keys (CVE-2013-3619)
CGI: logout.cgi (CVE-2013-3622)

SMT_X9_315, SMT X8 312
Hardcoded WSMan Credentials (CVE-2013-3620)
CGI: login.cgi (CVE-2013-3621)
CGI: close_window.cgi (CVE-2013-3623)
Stack-based Buffer Overflow (CVE-2013-3607)
Improper Input Validation (CVE-2013-3608)
Improper Privilege Management (CVE-2013-3609)

Check the following FAQ link for CVE-2013-4782
http://www.supermicro.com/support/faqs/faq.cfm?faq=16536

Note: Supermicro is currently testing the fix for CVE-2015-0235 (glibc library) and will update once the testing is finished.

Copyright © 2015 Super Micro Computer, Inc. – All Rights Reserved

CVE-2015-0291 CVE-2015-0204 is being investigated. We will update you on the availability of the fix (if affected).

BIOS Firmware Security Fixes:

NVRAM Protection (CVE-2014-8271): Not Affected

Romley - BIOS Rev 3.2, Denlow, SharkBay, Bromolow - BIOS Rev 2.2, Avoton, BayTrail, HSW-DT – BIOS Rev 1.2, Grantley BIOS Rev 1.0

Capsule Overflow (CVE-2014-4859, CVE-2014-4860)
Proper Flash Protection (CVE-2014-8273)
S3 Boot Script protection (CVE-2014-8274)- [Affected Grantley models with build date later than 01/13/2015]
UEFI Variable Security (CVE-2014-2961)

Note: Supermicro is investigating CVE-2015-0949. We will update you on the availability of the fix (if affected).

For further questions, please contact support@supermicro.com

Copyright © 2015 Super Micro Computer, Inc. – All Rights Reserved