Security Advisory Report - OBSO-1412-03

Hardening of the Intelligent Platform Management Interface (IPMI) on Unify Servers

Creation Date: 2014-12-31
Last Update: 2014-12-31

Summary

This is an informational advisory to address the need for proper hardening of the Intelligent Platform Management Interface (IPMI) on Unify servers. IPMI is implemented on a server's Baseboard Management Controller (BMC) and provides low-level remote access over IP for monitoring and managing the server, thus potentially allowing full control over the server and the operating system and applications running on it.

Server vendors implement IPMI as individual BMC firmware, such as IMM (IBM system x3550) or iRMC (Fujitsu RX200/RX330).
Associated IPMI hardening information for these two server types is available in the Security Checklists for OpenScape Voice V7 R1 and V8.

Vulnerability Details

The IPMI specification was originally defined by Intel as a standardized interface to the platform management subsystem of a server, called the Baseboard Management Controller (BMC).
IPMI is primarily used to remotely monitor the health of the system hardware. This typically includes monitoring elements such as system temperatures, voltages, fans, power supplies, bus errors, but also provides full access to system memory and I/O space.

The BMC is an independent embedded computer, integrated on most motherboards of today's server hardware. It is equipped with own CPU, RAM and storage, uses its own or the server's Ethernet interface to be accessible via IP (UDP port 623, plus vendor-specific TCP services such as 22/sshd, 80/http, 443/https), and continues to run even if the power switch is turned off.

Attackers could easily identify and access systems that expose the IPMI to untrusted or unmanaged networks. It is therefore important to

- restrict IPMI access to specific management IP addresses within an organization, preferably separated into a separate LAN segment
- apply additional hardening measures to prevent from potential misuse

Note that the IPMI 2.0 specification also includes a *"cipher 0"* configuration, that allows authentication to be bypassed. The hardening recommendations include information about the solution or mitigation of the cipher 0 configuration.

OpenScape Voice dual node installations make use of the IPMI interface to shut down the other node when triggered via the SA (Survivability Authority). Comprehensive hardening recommendations are therefore provided in the OpenScape Voice security checklists, covering both Fujitsu iRMC and IBM IMM firmware.

Affected Products

- OpenScape Voice servers in dual node deployment with Survivability Authority (SA)
- Potentially any other setup of IBM system x3550 or Fujitsu RX200/RX330 servers where Unify appliances or applications are installed on

Recommended Actions

In all cases where the IPMI interface over IP is enabled, the hardening steps are recommended as outlined in one of the following documents:

- Security Checklist OpenScape Voice V7 R1: chapter 3.4.5
- Security Checklist OpenScape Voice V8: chapter 3.4.13

Special notes for Fujitsu servers:

- On RX200 servers, ensure to use iRMC firmware version 6.55A or later, that have the cipher 0 option disabled
- For RX330 servers, there is no firmware version available, that disables cipher 0 completely. Instead, set the privilege level 'callback' for cipher 0 to prevent from unauthenticated IPMI logins

Special notes for IBM x3550 M2/M3 servers:

- To disable IPMI cipher 0 configuration, ensure that the IMM firmware is on version 1.42 or later
- Configure "high security mode" to disable weak TLS ciphers at the IMM's https interface
- For OpenScape Voice servers, appropriate updates were released as part of
  - MOP Q3056 in V7 R1.36.17 (release date 2014-10-10)
  - MOP Q3054 in V8 R0.26.7 (release date 2014-10-17)

References

Unify:

- Security Checklists for OpenScape Voice

Server vendor information:

- Intel: IPMI Specification
- Fujitsu: iRMC User Guides at http://manuals.ts.fujitsu.com/; direct links:
  iRMC S1 (for RX330 servers) and *iRMC S2/S3* (for RX200 servers)
- IBM: IMM/IMM2 User Guides at IBM Support Portal, direct links:
  IMM User Guide (for x3550 M2/M3 servers) and *IMM2 User Guide* (for x3550 M4 servers)

IPMI security in general:

- http://www.us-cert.gov/ncas/alerts/TA13-207A
- http://fish2.com/ipmi/

IPMI ciphersuite zero vulnerability and weak ciphers:

- CVE-2014-4030 for IBM IMM
- tenable.com: various CVE numbers related to the 'ciphersuite 0' vulnerability for different vendors

Revision History

2014-12-31: Initial release

Advisory ID: OBSO-1412-03 (a=76), status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer
OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com