安全产品关于IPMI v2.0密码哈希泄露漏洞的说明

漏洞相关 刘昆 2023-07-27 发表

漏洞相关信息

漏洞编号：无
漏洞名称：IPMI v2.0密码哈希泄露漏洞
产品型号及版本：安管一体机

漏洞描述

安全产品中的服务器，比如安管一体机、态势感知等产品用漏扫扫描出了高危漏洞，漏洞名称是“IPMI v2.0密码哈希泄露漏洞”。

此漏洞主要是IPMI2.0协议支持RMCP+机制引入导致，远程攻击者可以将HDM响应的RAKP包中密码的哈希值抓取，从而实施离线口令猜测攻击。该漏洞是协议机制导致，软件层面无法去修复，相关描述如下图说明。

漏洞信息详情

IPMI RMCP+ Authenticated Key-Exchange Protocol 安全漏洞

CNNVD编号：CNNVD-201307-123
CVE编号：CVE-2013-4786
发布时间：2013-07-09
更新时间：2013-07-09
漏洞来源：
危害等级：高危
漏洞类型：信任管理
威胁类型：远程
厂商：intel

漏洞简介

IPMI (Intelligent Platform Management Interface, 智能平台管理接口) 是美国英特尔 (Intel)、戴尔 (DELL)、惠普 (HP) 及日本NEC公司共同推出的一个使硬件管理具备“智能化”的新一代通用接口标准，它提供监视、控制和自动汇报大量服务器的运作状况的功能。

IPMI 2.0版本规范支持的RMCP+ Authenticated Key-Exchange Protocol (RAKP)身份认证中存在漏洞。远程攻击者可通过获得来自BMC响应的RAKP消息中的HMAC，利用该漏洞获得密码哈希值，实施离线口令猜测攻击。

漏洞公告

目前厂商还没有提供此漏洞的相关补丁或者升级程序，建议使用此软件的用户随时关注厂商的主页以获取最新版本：
<https://community.rapid7.com/community/metasploit/blog/2013/07/02/a-penetration-testers-guide-to-ipmi>

参考网址

来源: community.rapid7.com
链接: <https://community.rapid7.com/community/metasploit/blog/2013/07/02/a-penetration-testers-guide-to-ipmi>
来源: fish2.com
链接: <http://fish2.com/ipmi/remote-pw-cracking.html>

受影响实体

● Intel Intelligent_platform_management_interface:2.0

来源：国家信息安全漏洞库

实际测试各大服务器厂商均没有修复此漏洞，测试结果如下图：

The screenshot shows a vulnerability scanner interface. At the top, it displays the user 'youshang' and the IP address '172.16.16.200'. Below this, there are buttons for 'Configure', 'Audit Trail', 'Launch', and 'Report'. A search bar contains the text 'IPMI v2.0 Password Hash Disclosure'. Below the search bar, a table lists the search results. The table has columns for 'Severity', 'Name', 'Family', 'Count', and 'Host Details'. One result is shown: 'IPMI v2.0 Password Hash Disclosure' with a severity of 'High', a count of '2', and host details for IP '172.16.16.200' and MAC '5050:AC:05:08:08'.

友商测试结果和H3C我司结果一致。

漏洞解决方案

规避措施:

如果管理网IP (HDM) 没有直接连接到公网, 此漏洞被利用的风险极小; 建议管理网不在公网暴露IP

。

如果管理网IP(HDM) 是暴露在公网中, 那么建议如下方式:

方法一, 增加密码复杂度, 避免使用弱密码。

方法二, 增加白名单访问机制, 其次将已知的访问源IP都增加到白名单, 这样能有效遏制恶意攻击源

。

方法三, 如果纳管不是基于IPMI over LAN的, 那么可以通过HDM页面关闭IPMI端口, 漏洞不会再对外暴露, 也无法被扫描到。

服务设置

名称	状态	接口	非安全端口	安全端口	超时	最大会话	操作
CD-Media	开启	both	5120	5124	N/A	2	查看 修改
FD-Media	开启	both	5122	5126	N/A	1	查看 修改
HD-Media	开启	both	5123	5127	N/A	2	查看 修改
IPMI	禁用	N/A	623	N/A	N/A	N/A	查看 修改
KVM	开启	both	7578	7582	30	4	查看 修改
Remote_XDP	禁用	N/A	6868	N/A	N/A	1	查看 修改
SNMP	开启	N/A	161	N/A	N/A	N/A	查看 修改