# [Windows 更新 BIOS 方法與步驟]

## [擎昊科技工程部專用]

2018 年 1 月 11 日 撰寫人: 沈劭嶸、姜柏任

 Kinmax

 KINMAX TECHNOLOGY INC

 擎昊科技股份有限公司

 電話:03-6562709

 免費諮詢專線:0800-046629

 服務信箱:service.hc@kx.com.tw

 公司地址:新竹縣竹北市縣政九路 147 號 5 樓



## [Windows 更新 BIOS 方法與步驟]

#### 內容

1.	說明	2
2.	影響	2
3.	HPE 解決方法	2
	ONLINE-進入系統利用工具包更新 BIOS FIRMWARE	2
	ILO – 利用 PROLIANT SERVER 中的 ILO 來更新 BIOS FIRMWARE	2
4.	PROLIANT GEN9 BIOS FIRMWARE 載點 & 文件	2
5.	ONLINE 更新 FIRMWARE 方法與步驟	4
6.	ILO 更新 FIRMWARE 方法與步驟	9

#### 1. 說明

過去 10 年中的英特爾處理器(CPU),存在嚴重的晶片級安全漏洞,是 「現代的設計缺陷」,該漏洞允許用戶程式辨別受保護內存記憶體的內容, 駭客可以利用這個缺點更容易地發現其他安全漏洞。

Kínmax

擎昊科技股份有限公司

#### 2. 影響

目前微軟 Windows 和 Linux 開發人員已經開始著手進行修復,但更新後會 繞過一些 CPU 架構,會對英特爾的產品性能產生衝擊,可能會降速 2%至 30%,大部分的電腦則是 2%至 4%,若系統上的應用有大量與作業系統互動 的複合式工作負載,效能下降的程度會更高。

#### HPE 解決方法

HPE 原廠提供更新 BIOS Firmware 來修復英特爾(Intel)漏洞的問題

- Online 進入系統利用工具包更新 BIOS Firmware
- iLo 利用 ProLiant Server 中的 iLo 來更新 BIOS Firmware

#### 3. ProLiant Gen9 BIOS Firmware 載點 & 文件

For ProLiant Gen9 series servers, update to System ROM Version 2.54 (except for the ProLiant DL20 Gen9 or ML30 Gen9) For the ProLiant DL20 Gen9 or ProLiant ML30 Gen9 server, update to System ROM Version 2.52.

#### HPE 文件

https://support.hpe.com/hpsc/doc/public/display?docId=emr\_na-a00039267en\_us

#### Firmware

https://support.hpe.com/hpsc/swd/public/detail?swItemId=MTX\_cf6657e373254295b51b2e368a#tabhistory



2. 左側選擇 OS 版本及 Software Type,就會篩選出相關軟體並點擊進入下載頁面。



3. 確認版本及 OS 支援沒有問題,即可下載。



### 4. Online 更新 Firmware 方法與步驟

#### 1. 可先利用 PowerShell 執行 msinfo32 確認系統 BIOS 版本 IO Integrated Remote Console - Server: WIN-CCC47NUBITK | iLO: ILOSGH747V8PS Power Switch Virtual Drives Keyboard Help \_ \_ × 系統管理員: Windows PowerShell soft Corporation. 著作権 ws PowerShell著作權(C)2013 Mi 著作権) 条統資訊 - 0 檔案(F) 編輯(E) 檢視(V) 說明(H) 項目 OS 名稱 版本 其他作業系統指述 OS 販賣 未統型語 系統型語 未統型語 未統型語 素統型語 BIOS 成本 BIOS 成本 BIOS 成本 <u>●統備要</u> 由-硬體資源 由-元件 由-款體環境 酒日 6.3.9600 組建 9600 無法使用 Microsoft Corporation WIN-CCC47NUBITK HP ProLlant DL380 Gen9 x64 PC 719064-821 Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz + 2098 Mhz + 8 價核心 HP P89, 2017/12/7 28 2.8 2.54 UEFI BIOS 模式 BaseBoard 製造商 BaseBoard 型號 BaseBoard 名稱 平台角色 安全開機狀態 PCR7 設定 Windows 目錄 表紙目錄 開機裝置 UEFI HP 無法使用 立葉伺服器 範閱 無法使用 C:\Windows C:\Windows\system32 \Device\HarddiskVolume2 地面設定 台灣 ш 尋找目標(W): 尋找(D) 關閉尋找(C) 只搜尋已選取的類別(S) □ 只搜尋類別名稱(<u>R</u>) T- $\geq$ Po 😼 😘 ቀ 2018/1/1 1024 x 768 H II > • 🔒 RC4 🛛 🔿 🕲 🥹

[Windows 更新 BIOS 方法與步驟 ] | 2018/1/11

2. 從載點下載檔案至 Server

Kínmax

擎昊科技股份有限公司

io iLO Integrated Remote Console - iLO: ILOSGH747V8PS	
Power Switch Virtual Drives Keyboard Help	
Power switch "Witcar Dives" Keyddard" Help 算源回收截 cp034250	
	Windows Server 2012 R2
	Windows Server 2012 R2 Standard
	- 10日 9500 - 10日 9500 - 10日 9500
1024 x 768	

3.將檔案以系統管理員學	<b>身分執行</b>
iiO Integrated Remote Console - iLO: ILOSGH747V8PS	
Power Switch Virtual Drives Keyboard Help	
<b>宣</b> 涛回收简	
開啟(0)	
cp0342	
疑難排解相密性(V)	
刻 編到開始 亜田(P)	
(H) 秋用町率(H) ・	
還原舊版(V)	
傳送到(N) ▶	
剪下(T)	
複製(C)	
建立捷徑(S)	
<b>刪除(D)</b>	
里新部名(M)	
内魯(R)	
	Hereit Windows Server 2012 R2
	Windows Server 2012 R2 Standard Build 9600
	▲ 🖻 😼 🥶 つわけなけ
1024 x 768	× = = = = = = = = = = = = = = = = = = =

[Windows 更新 BIOS 方法與步驟 ] | 2018/1/11

4.確認更新版本為 2.54 -> 選擇 Install

Kínmax

擎昊科技股份有限公司





[Windows 更新 BIOS 方法與步驟] | 2018/1/11



6.開始更新		
iLO Integrated Remote Console - iLO: ILOSGH747V8PS		23
Power Switch Virtual Drives Keyboard Help		
黄源回收筒		
ep034250		
	彩 Setup	
	Online ROM Flash Component for Windows x64 - HPE ProLiant DL380 Gen9/DL360 Gen9 (P89) Servers Software Versior: 254 (12/07/2017)	
Managem	The installation is being performed at this time. Please wait until the operation completes	
	Windows Server 2012 R2	
	Windows Server 2012 R2 Standa Build 90	ard 500
	▲ 10	1
1024 x 768	🕷 n (k e) 🗳 RC4 🌒	• •



8.需要重新啟動 Server 才能套用 Firmware -> 選擇 "是", 或是另擇日重啟。

[Windows 更新 BIOS 方法與步驟] | 2018/1/11

7

Kinmax

擎昊科技股份有限公司

iLO Integrated Remote Console - iLO: ILOSGH747V8PS		23
Power Switch Virtual Drives Keyboard Help 實際回收商 cp-034250		
HPE System Managem	Package Setup	
O - I S V Th International	A reboot is required to finish the installation completely. Do you want to reboot your system now? State Table Completely Completel	
	Windows Server 2012 R2	
	Windows Server 2012 R2 Star Build ▲ IP 溜 ゆ ② 5年の 2015/	ndard 9600 6:43 1/11
1024 x 768	11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	

HPEE ProLiant       Fewlett Packard         (C) Copyright 1982 - 2017 Hewlett Packard Enterprise Development LP       Forceason         (D) Copyright 1982 - 2017 Hewlett Packard Enterprise Development LP       Forceason         (D) Copyright 1982 - 2017 Hewlett Packard Enterprise Development LP       Forceason         (D) Copyright 1982 - 2017 Hewlett Packard Enterprise Development LP       Forceason         (D) Copyright 1982 - 2017 Hewlett Packard Enterprise Development LP       Forceason         (D) Copyright 1982 - 2017 Hewlett Packard Enterprise Development LP       Forceason         (D) Copyright 1982 - 2017 Hewlett Packard Enterprise Development LP       Forceason         (D) Copyright 1982 - 2017 Hewlett Packard Enterprise Development LP       Forceason         (D) Copyright 1982 - 2017 Hewlett Packard Enterprise Development LP       Forceason         (D) Copyright 1982 - 2017 Hewlett Packard Enterprise Development LP       Forceason         (P) Proceason (S) detected - 16 total cores enabled. Hyperthreading is enabled       Forceason         (P) Power Profile Mode: Maximum Performance       Forceason         (P) Power Profile Mode: Static High Performance       Forceason         (P) Power Regulator Mode: Static High Performance       Forceason         (P) Power Regulator Mode: IPP       Forceason         (P) Power Regulator Mode: IPP       Forceason         (P) Power Regulator Mode: IPP </th <th>ILO Integrated Kemote Console - ILO: ILOSGH /4 /V8/S wer Switch Virtual Drives Keyboard Help</th> <th></th> <th></th>	ILO Integrated Kemote Console - ILO: ILOSGH /4 /V8/S wer Switch Virtual Drives Keyboard Help		
CC) Copuright 1982 - 2017 Hewlett Packard Enterprise Development LP       IP Proliant DL380 Geng         IDOS Version: P089 v2.54 (12/07/2017)         Serial Number: SGH74708PS         System Memory: 32 GB         2 Processor G3 detected, 16 total cores enabled, Hyperthreading is enabled         froc 1: Intel (8) Keon (8) CPU E5-2620 v4 @ 2.10GHz         froc 2: Intel (8) Keon (8) CPU E5-2620 v4 @ 2.10GHz         froc 2: Intel (8) Keon (8) CPU E5-2620 v4 @ 2.10GHz         froc 3: Intel (8) Keon (8) CPU E5-2620 v4 @ 2.10GHz         froc 4: Intel (6) Keon (8) CPU E5-2620 v4 @ 2.10GHz         froc 4: Intel (6) Keon (8) CPU E5-2620 v4 @ 2.10GHz         froc 5: Intel (6) Keon (8) CPU E5-2620 v4 @ 2.10GHz         froc 4: Intel (6) Keon (8) CPU E5-2620 v4 @ 2.10GHz         froc 4: Intel (6) Keon (8) CPU E5-2620 v4 @ 2.10GHz         froc 5: Intel (6) Keon (8) CPU E5-2620 v4 @ 2.10GHz         froc 6: Intel (6) Kaon (8) CPU E5-2620 v4 @ 2.10GHz         froc 6: Intel (6) Kaon (8) CPU E5-2620 v4 @ 2.10GHz         froc 7: Intel (6) Keon (8) CPU E5-2620 v4 @ 2.10GHz         froc 6: Intel (6) Made: Static High Performance         Newarce Regulator Mode: Static High Performance         Newarce Regulator Mode: Static High Performance         Short Mode: UEFI         Redundant ROM Detected - This system contains a valid backup system ROM         IPE REGULAR ALL HIGH ALL HIGH ALL HIGH ALL HIGH ALL HIGHT	HPE ProLiant	Hev Ent	<b>Niett Packar</b> erprise
Augstem Memory: 32 GB 2 Processor G3 detected, 16 total cores enabled, Hyperthreading is enabled Proc 1: Intel(R) Keon(R) CPU E5-2620 v4 @ 2.10GHz Proc 2: Intel(R) Keon(R) CPU E5-2620 v4 @ 2.10GHz Proc 1: Intel(R) Keon(R) CPU E5-2620 v4 @ 2.10GHz Proc 2000 v4 @ 2.10GHz Pro	CC) Copyright 1982 - 2017 Hewlett Packard Enterprise Development LP HP Proliant DL380 Gen9 HOS Version: P89 v2.54 (12/07/2017) Serial Number: Scht41708PS		
IPE Power Profile Mode: Maximum Performance         Yower Regulator Mode: Static High Performance         Novanced Memory Protection Mode: Advanced ECC Support         Inlet Ambient Temperature: 25°C / 77°F         Noot Mode: UEFI         Redundant ROM Detected - This system contains a valid backup system ROM         IPE SmartMemory authenticated in all populated DIMM slots.         Starting drivers. Please wait, this may take a few moments         IO 4 IPv4: 192.168.79.223         ID 4 IPv6: FE80:: 90F2:B3FF:FE2E: 9E02	ystem Memory: 32 GB ? Processor(s) detected, 16 total cores enabled, Hyperthreading is enabled froc 1: Intel(R) Keon(R) CPU E5-2620 v4 @ 2.10GHz froc 2: Intel(R) Keon(R) CPU E5-2620 v4 @ 2.10GHz PI Speed: 8.0 GT/s	4777 8 4 4778 8 4 4788 8 4 4	
Redundant ROM Detected - This system contains a valid backup system ROM       Image: Smart Array Starting drivers. Please valt, this may take a few moments       Image: Smart Array Starting drivers. Please valt, this may take a few moments       Image: Smart Array	IPE Power Profile Mode: Maximum Performance Power Regulator Mode: Static High Performance Idvanced Memory Protection Mode: Advanced ECC Support Inlet Ambient Temperature: 25°C / 77°F Boot Mode: UEFI		
tarting drivers. Please wait, this may take a few moments Power Regulator LO 4 IPv4: 192.168.79.223 LO 4 IPv6: FE80::9AF2:B3FF:FE2E:9E02	edundant ROM Detected - This system contains a valid backup system ROM IPE SmartMemory authenticated in all populated DIMM slots.		Smart Storage Smart A Battery
LO 4 IPu4: 192.168.79.223 LO 4 IPu6: FE80::9AF2:B3FF:FE2E:9E02 HPE RESTINI API Provisioning 30	itarting drivers. Please wait, this may take a few moments	Power Regulator	Dynamic HPE Power Capping SmartNe
	LO 4 IPv4: 192.168.79.223 LO 4 IPv6: FE80::9AF2:B3FF:FE2E:9E02	HPE RESTIU API	Intelligent Sea of Se Provisioning 3D



#### 5. iLo 更新 Firmware 方法與步驟



[Windows 更新 BIOS 方法與步驟 ] | 2018/1/11



擎昊科技股份有限公司

2.選擇 Admi	nistrator 的 Firmware -> 選擇瀏覽來上傳 BIOS Firmware 檔案
Hewlett Packard Enterprise	ILO 4 Local User: administrator ProLlant DL380 Gen9 LOSGH749XP7V.
Expand All	Firmware Update
> Virtual Media	^
> Power Management	Obtain the firmware image (.bin) file from the Online ROM Flash Component for HPE iLO 4.
> Network	<ul> <li>The latest component can be downloaded from http://www.hpe.com/support/ilo4.</li> <li>This component is also available on the HPE Service Pack.</li> </ul>
✓ Remote Support	Server Firmware
Registration	
Service Events	The following types of server firmware can also be updated from this page:
Data Collections	
✓ Administration Firmware	HPE System ROM     System Programmable Logic Device     SL/XL Chassis Firmware
Licensing	Server firmware files can be obtained from http://www.hpe.com/support/ilo4. For more information, please see the help file.
User Administration	
Access Settings	Local File: Update the firmware by uploading a local file. Note: Navigating away from this page before the upload has completed will prevent the update from starting.
Security	File
Management	100. <u>2019</u>



[Windows 更新 BIOS 方法與步驟]| 2018/1/11

Kínmax

擎昊科技股份有限公司

#### 4.選擇 Upload 開始更新 Hewlett Packard iLO 4 Local User: administrator iLO Hostname: ILOSGH749XP7V. Firmware Update Group Configuration ^ Obtain the firmware image (.bin) file from the Online ROM Flash Component for HPE iLO 4. ✓ Remote Console The latest component can be downloaded from http://www.hpe.com/support/ilo4. This component is also available on the HPE Service Pack. Remote Console > Virtual Media Server Firmware > Power Management > Network The following types of server firmware can also be updated from this page: > Remote Support HPE System ROM System Programmable Logic Device SL/XL Chassis Firmware Administration Server firmware files can be obtained from http://www.hpe.com/support/ilo4. For more information, please see the help file. Licensing User Administration Access Settings Local File: Update the firmware by uploading a local file. Note: Navigating away from this page before the upload has completed will prevent the update from starting. Security C:\Users\ASUS\Downloads\cp034250\P89\_2.54\_12\_07 瀏覽... File: Management Key Manager iLO Federation Upload DOWER: ON 🖗 UID: BLIN

ewlett Packard hterprise		ILO 4 ProLiant DL380 Gen9				Local User: administ iLO Hostname: ILOSGH749XI	ator HOME 27V.	SIG
kpand All		LO Overview						
Information	~	Information			Status			
Overview System Information iLO Event Log Integrated Management Log Active Health System Log Diagnostics Location Discovery Services		Server Name Product Name UUID Server Serial Number Product ID System ROM System ROM Date Backup System ROM	ProLiant DL380 Gen9 30393137-3436-4753-4837-343958503756 SGH749XP7V 719064-B21 P89 v2.52 (10/25/2017) 10/25/2017 10/25/2017		System Health Server Power UID Indicator TPM Status SD-Card Statu ILO Date/Time Connection	<ul> <li>OK</li> <li>ON</li> <li>UID BLINK</li> <li>Not Present</li> <li>Not Present</li> <li>Thu Jan 11 06:26:51 2018</li> <li>to HPE</li> </ul>		
Insight Agent		License Type	iLO Advanced Evaluation		🔺 Not regi	stered		
iLO Federation Remote Console		iLO Firmware Version IP Address	2.55 Aug 16 2017 192.168.79.48					
Remote Console		Link-Local IPv6 Address iLO Hostname	FE80::9AF2:B3FF:FE2E:3F0A ILOSGH749XP7V.					
Virtual Media								
Power Management								
Network		Active Sessions						
Remote Support	~	User Local User: administrator		▲ IP Address 192.168.39.99		Source HTTPS		

6.更新完成後請記得重開機才會生效,檢查開機畫面,BIOS 是否更新完成

[Windows 更新 BIOS 方法與步驟]| 2018/1/11



Hewlett Packard Interprise	iLO 4 ProLiant DL380 Gen9				
Expand All	iLO Overview				
Information	Information			Status	
System Information	Server Name Product Name	ProLiant DL380 Gen9		System Health Server Power	<ul> <li>ОК</li> <li>ОN</li> </ul>
iLO Event Log	UUID	30393137-3436-4753-4837-343958503756		UID Indicator	VID BLINK
Integrated Management Log	Server Serial Number	SGH749XP7V		TPM Status	Not Present
Active Health System Log	Product ID System ROM	/19064-B21 P89 v2 54 (12/07/2017)		SD-Card Status	Not Present Thu Jan 11 06:28:41 201
Diagnostics	System ROM Date	12/07/2017			
Location Discovery Services	Backup System ROM	10/25/2017		Connection to	o HPE
Insight Agent	Integrated Remote Console	.NET Java Web Start Java Applet		A Not registe	ared
ILO Federation	iLO Firmware Version	2.55 Aug 16 2017		Mot registe	sieu
Remote Console	IP Address	192.168.79.48			
Virtual Media	Link-Local IPv6 Address	FE80::9AF2:B3FF:FE2E:3F0A			
Power Management	ico rioduane				
> Network					
Remote Support	Active Sessions				
Administration	User Local User: administrator		<ul> <li>IP Address</li> <li>192.168.39.99</li> </ul>		Source HTTPS

[Windows 更新 BIOS 方法與步驟 ] | 2018/1/11



≥ 13