آسیب‌پذیری بحرانی برروی محصول ESXi شرکت VMware با شماره CVE-2019-5544

این آسیب‌پذیری در سرویس OpenSLP محصول ESXi مشاهده شده است. سرویس SLP بصورت پیش‌فرض برروی درگاه 427 فعال است. آسیب پذیری مذکور امکان اجرای کد از راه دور را برای مهاجم، بدون نیاز به هیچ دسترسی، فراهم می‌کند. ضعف این آسیب‌پذیری از نوع Heap Buffer Overflow و با شماره CWE-122 بوده و رتبه‌ی CVSS آن برابر ۹٫۸ می‌باشد.

نسخه‌های 6.0 و 6.5 و 6.7 سرویس‌دهنده‌های ESXi و همچنین سرویس Horizon DaaS 8.x دارایی این آسیب‌پذیری می‌باشند.

راهکار پیشنهادی:

بهترین روش برای پیشگیری از وقوع حمله سایبری از طریق این حفره امنیتی، بروز رسانی سرویس‌دهنده‌ی ESXi می‌باشد. شرکت VMware وصله امنیتی برای برطرف سازی این آسیب‌پذیری ارائه نموده‌است، که در لینک زیر قابل دریافت است:

https://my.vmware.com/group/vmware/patch

همچنین در صورت اطمینان خاطر و عدم نیاز، می‌توانید سرویس SLP را بصورت موقتی با دستور زیر متوقف نمود.

```
/etc/init.d/slpd stop
```

درصورتی که سرویس SLP در حال استفاده توسط فرآیندی باشد امکان متوقف سازی آن وجود ندارد. با اجرای این دستور می‌توان وضعیت این سرویس را مشاهد نمود.

```
esxcli system slp stats get
```

با استفاده از دستور زیر می‌توانید سرویس SLP را هم غیر فعال نمود.

```
esxcli network firewall ruleset set -r CIMSLP -e 0
```

برای اینکه تغییرات پس از reboot نیز پایدار بمانند از دستور زیر استفاده گردد.

```
chkconfig slpd off
```

منابع :

https://www.vmware.com/security/advisories/VMSA-2019-0022.html

https://kb.vmware.com/s/article/76411

https://www.securityweek.com/vmware-patches-esxi-vulnerability-earned-hacker-200000