New Microsoft Security ?Nightmare?: Users Warned Your Passwords Are Now At Risk

Microsoft security is under fire after new research, published here for the first time, exposes the serious risk of account hijack from compromised subdomains. Put simply, users visiting a genuine Microsoft web domain might actually be on a subdomain controlled by an attacker. Any information those users then share will be at risk?including usernames and passwords. Users are advised to take care the links they click, but if subdomains appear genuine, they will likely be tricked.

"We are aware of such reports,? a Microsoft spokesperson told me, ?and are taking appropriate action as needed to help protect services and customers." While the lack of controls on Microsoft subdomains has been exposed before, this new report from Numan Ozdemir and Ozan Agdepe of Vullnerability.com includes a proof of concept video (see below) that shows how simple this is in practice.

There are no claims that these exploits have been exploited in the wild yet. But the vulnerability is now in the public domain. It is only a matter of time before bad actors seek to exploit the issue and put users at risk. ?Enterprise sprawl and a lack of internal domain controls has created a nightmare,? cyber expert Ian Thornton-Trump tells me. ?I suspect in the wake of this, Microsoft will need to implement significant changes in how domains are managed.?

Cumulative Update 2 for Microsoft SQL Server 2019 breaks SQL Server Agent

Microsoft has admitted that Cumulative Update 2 for SQL Server 2019 has a problem, and
those using SQL Server Agent should either skip it or roll it back.

Cumulative Update 2 appeared on 13 February and contains all manner of important fixes for database botherers aimed at boosting performance and improving stability.

Alas, things seemed to go wrong pretty quickly for some database admins as users took to the DBA forums in StackExchange to complain that the SQL Server Agent seemed a bit poorly after applying the update.

Seemingly random failures, problems with schedules and freezes were mentioned as users struggled to get to grips with what was going wrong. Microsoft's own forums were similarly blighted, with one user making the important point: "In addition to not showing jobs they are also not being run so important jobs such as backups aren't being done."

SQL Server Agent is responsible for running jobs such as backups and other maintenance tasks. It can also be found running T-SQL for all manner of purposes, so for it to be broken is not ideal.


A sophisticated hacker group pwned Amazon Web Services (AWS) servers, set up a rootkit that let them remotely control servers, then merrily funnelled sensitive corporate data home to its command and control (C2) servers from a range of compromised Windows and Linux machines inside an AWS data centre.

That's according to a report from the UK's Sophos published late last week, which has raised eyebrows and questions in the security industry. The attackers neatly sidestepped AWS security groups (SGs); which, when correctly configured, act as a security perimeter for associated Amazon EC2 instances.

The unnamed target of this attack had correctly tuned their SGs. But with a rootkit installed on their AWS servers that gave attackers remote access, the compromised Linux system was still listening for inbound connections on ports 2080/TCP and 2053/TCP: something that eventually triggered Sophos' intervention.

Intel x86 Root of Trust: loss of trust [5]

The scenario that Intel system architects, engineers, and security specialists perhaps feared most is now a reality. A vulnerability has been found in the ROM of the Intel Converged Security and Management Engine (CSME). This vulnerability jeopardizes everything Intel has done to build the root of trust and lay a solid security foundation on the company's platforms. The problem is not only that it is impossible to fix firmware errors that are hard-coded in the Mask ROM of microprocessors and chipsets. The larger worry is that, because this
vulnerability allows a compromise at the hardware level, it destroys the chain of trust for the
platform as a whole.

Positive Technologies specialists have discovered an error in Intel hardware, as well as an
error in Intel CSME firmware at the very early stages of the subsystem's operation, in its boot
ROM. Intel CSME is responsible for initial authentication of Intel-based systems by loading
and verifying all other firmware for modern platforms. For instance, Intel CSME interacts with
CPU microcode to authenticate UEFI BIOS firmware using BootGuard. Intel CSME also
loads and verifies the firmware of the Power Management Controller responsible for
supplying power to Intel chipset components.

•

Intel x86 Root of Trust: loss of trust [6]

The Positive Technologies blog is reporting on an unfixable flaw the company has found in
Intel x86 hardware that has the potential to subvert the hardware root of trust for a variety of
processors.

Security

Source URL: http://www.tuxmachines.org/node/134853

Links:
[6] https://lwn.net/Articles/813943/rss