TREND MICRO™

Securing Your Journey to the Cloud

The Olympics change freeze:
Don't leave your critical systems out in the cold

By **John Burroughs**, CISSP Senior Solutions Architect

Most organisations operate a change freeze on their IT systems as a control for managing risk and keeping a stable and available IT environment around critical times of the year. However, this strategy can introduce an even greater risk to business operations. Each year thousands of vulnerable software flaws are reported in operating systems and applications that are being exploited.

This paper explains how you can implement same-day protection for vulnerabilities whilst still maintaining your Change Freeze.

Dani King, 2011 World & European Team Pursuit Champion. **Sponsored by Trend Micro.**

Getting ready for the big freeze

The Olympics Games will be held in the UK from July 27 to August 12, and with venues in and around London and the whole country, a range of nationwide organisations, including government, emergency services, transport and other key agencies, are implementing a range of programmes to ensure they are able to react quickly and efficiently to incidents.

"Policing the Games will present the force with an unprecedented challenge. As well as physical threats, a global scale event like the Olympics will be a potential hotbed for cybercrime"

Tony Neate, Managing Director, Get Safe Online

In order that no disruptions or instability are introduced to critical systems during the games, many of these organisations will be operating a change freeze; a point in time after which no modifications or upgrades are allowed to occur to any systems or applications.

How change freezes work

An organisation's data centre is constantly changing. New network, hardware and software components are added and existing ones are patched, updated, re-configured and maintained. Any change made in the data centre can put the organisation at risk of operational disruption since a change might cause instabilities or even outages in their IT systems. Even though organisations will have tight processes and controls in place on how these changes are implemented, unexpected disruptions can still occur.

Any disruption to an organisation's IT systems which affect business is undesirable at the best of times; however, throughout critical periods like the Olympics, outages are simply unacceptable. Hence data centre change freezes will be implemented to ensure the integrity and availability of IT systems and minimise risk of business disruption.

The colder side of a change freeze

While a change freeze is put in place to maintain the stability of an organisation's IT systems, this approach can actually be putting the very same systems at even greater risk. Each year, thousands of vulnerable software flaws are reported in operating systems and applications that are being exploited by cybercriminals.

A Denial-of-service (DoS) attack could cripple the forces' communication systems

The number of publicly reported vulnerabilities in 2011 was 4,155[1] and those trends are going to continue in 2012 with attacks become increasingly complicated. Furthermore, major sporting events like the Olympics tend to draw large scale cyber attacks; during the 2008 Beijing Olympics, China suffered about 12 million online attacks per day.

In order to remediate these vulnerabilities, patches are deployed, however, a change freeze usually means that patching is put on hold, and this is where the greatest risk is introduced.

Patching is a security practice designed to prevent the exploitation of flaws in operating systems and applications, and mitigate vulnerabilities. Timely patching of vulnerabilities is critical to maintaining the availability and integrity of an organization's IT systems. This is because as soon as a patch is released, attackers can reverse engineer the patch, find the vulnerability and develop code to exploit it. And in some cases, this can happen within a matter of hours.

The window of vulnerability is the time between discovering a vulnerability and applying a patch to address it. It is when the business infrastructure lies open to attacks and is at its most vulnerable.

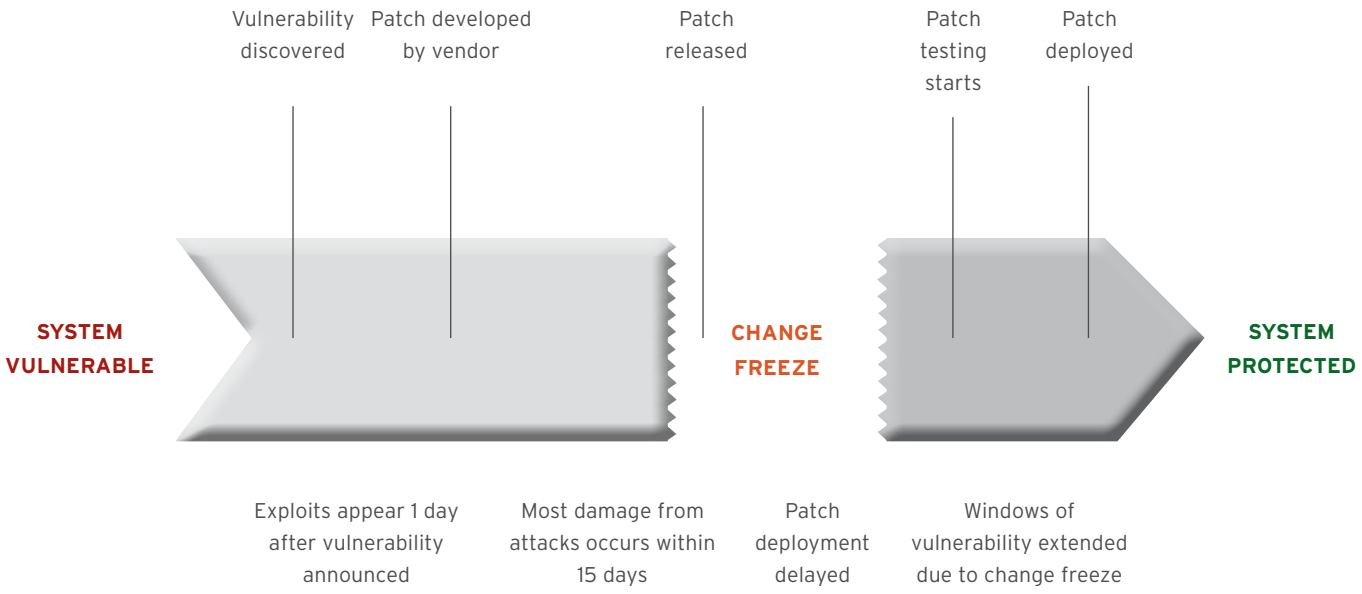
Conficker targeted the Microsoft Windows operating system and is the largest known computer worm infection since 2003. At its peak, it had infected an estimated seven million government, business and home computers in over 200 countries, causing users to be locked out, disabling of critical services and severe network congestion.

Patching is also a compliancy requirement, for example PCI-DSS mandates that critical systems within a cardholder data environment should be patched within 30 days. A change freeze can mean that an organization may become non-complaint with the regulations they need to adhere to.

All organisations realise the importance of properly patched systems, however, they face a dilemma. They need to be able to patch their systems but they cannot risk a disruption to their services. The Olympics pose an unprecedented challenge for all organisations involved and many will make the decision to maintain a stable environment at the cost of maintaining a secure environment.

[1] US National Vulnerability Database

Change Freeze Period means systems remained unpatched longer



The best defence

As we've discussed, change freezes can mitigate some risks whilst introducing new risks. But you can protect yourself with the right solutions and a few simple best practices.

The traditional method of applying permanent software patches and upgrading software is clearly challenging during a change freeze period such as will be seen during the Olympics. However, even outside of change freeze periods, this approach is too labour-intensive, costly and invasive to compete with the speed of exploits and to adequately protect the business.

You can easily and cost effectively deliver protection within hours of a vulnerability being announced with the right solution – even during a change freeze. Trend Micro Deep Security offers this alternative strategy through Virtual Patching, also known as vulnerability shielding, which proactively shields systems from attacks.

Trend Micro Deep Security does this by inspecting network traffic for malicious activity which is trying to exploit vulnerabilities in operating systems and applications. Once detected, alerts can be raised and action taken. This allows an organisation to apply protection to their systems without having to touch their running systems, not even a reboot is required. We can shield vulnerabilities in your critical systems, allowing you to achieve your change freeze objective while still maintaining the security and compliancy of your environment. Furthermore, this approach gives you visibility into attacks against your organisation which permanent patching and upgrading measures do not.

The alternatives?

Ensure you fully understand the implications of implementing a change freeze without virtual patching

- Understand where you are most vulnerable
- Continue to carry out ongoing vulnerability assessments and assess weakness throughout the period
- Evaluate your security posture in light of new vulnerabilities being discovered, for example, after every patch Tuesday
- Determine criteria for doing nothing versus reacting
- Establish a process, with appropriate escalation, for emergency patching
- Calculate the cost and risk of emergency patches and software fixes

TREND MICRO™

Securing Your Journey to the Cloud

Find out more about how virtual patching could reduce IT resources and costs while enhancing the security and compliance of data centre applications.

Call 01628 400552

ww.trendmicro.co.uk

Trend Micro (UK) Limited, a Limited Liability Company. Registered in England No. 3698292. Registered Office: Pacific House, Third Avenue, Globe Business Park, Marlow, Bucks, SL7 1YL