Silent Risk – Why We Must Upgrade Network Software

Your network runs smoothly? Keep it that way

By John N. Stewart, Vice President and Chief Security Officer, Cisco

Ask most company information security officers about enterprise security and we'll speak with conviction about threats to our desktop, data-center systems, and applications. We'll talk about our vigilant efforts to continuously secure those assets, possibly with a wry smile acknowledging the thought that our users are sometimes our biggest threat. What you rarely hear us mention is threats to the network devices themselves and the operating systems on which we rely. Unfortunately, this is our blind spot and a growing security threat for organizations of all sizes. A network running last year's OS is just not as secure as you might think, and within many organizations it gets less attention than it warrants. This is probably because, for the most part, it just works. But in truth, the longer a network goes without upgrades and attention, the longer the list of accumulated exploits to which it may be vulnerable. We've seen the threat against network operating systems grow substantially over the past decade.

Imagine that your network went down. You would likely lose access to mission-critical data, voice, video, and business applications. Your customers might be unable to contact you. Scarier yet, envision your network becoming an "insider threat," running smoothly while outside parties were using your network like a bot to steal and exploit your critical business information. Science fiction? Hardly.

Why are we not upgrading?

These days, network attack research increasingly makes news headlines. It may seem odd for me, an executive for a network vendor, to call attention to this issue. After all, with proactive marketing campaigns, a deep and broad set of security products, and actionable intelligence portals, Cisco is already committed to helping its customers protect themselves. However, you and I know that networking devices too frequently run older code and are weakened by doing so. If networks are essentially a conglomeration of computing devices with their operating systems, why are they routinely left untouched while business applications, desktop and server operating systems, and server hardware get regular maintenance and updates?

The answer lies, in part, with human nature. Let's face it, who wants to risk network downtime or introduce change into an infrastructure that runs smoothly when there are seemingly plenty of more pressing security risks? When network metrics are showing positive results, systems are running smoothly, nothing is failing, and auditors aren't causing a stir, why look into it at all?

Secondly, many IT professionals consider network OS software arcane. We are reading about common exploits for networking operating systems and beginning to hear about malware and a possible network OS virus, and maybe even imagining botnets that exploit routing devices. Is it easier to think that such things are still improbable? I suppose so, and yet, knowing the complexity inherent to any operating system, it isn't a matter of if these events will happen, rather when.

How often one should upgrade network software varies with the network size, complexity, security requirements, resource constraints, and other considerations. For most networks, twice a year is a good place to start, and annually should be considered a minimum.

Admittedly, upgrading a network isn't always an easy task. It may require new hardware or additional memory, scheduled downtime, and most definitely a fair amount of research and testing simply to determine the correct upgrade path. At Cisco, we are working diligently to simplify the upgrade process, yet recognize that there is a lot of room for improvement on our part.

Network upgrades enhance your security strategy

As I've asserted here, the network and IT systems make up an organization's most critical infrastructure. They are the conduit for data, voice, and video, providing "always on" customer service, and are frequently mission-critical in every sense. Unplanned network downtime is or is rapidly becoming unacceptable, so I submit that any enterprisewide security plan that ignores planned upgrades to the network is incomplete. Routine network upgrades are an essential element in every security and risk mitigation plan, and a well-thought-out security strategy is a critical component of the network's technical and operational architectures.

Upgrading to secure a network isn't just a defensive strategy. It's a proactive one that protects your business and provides necessary stability to your network. In addition to safeguarding a network from older attacks, human error, and natural disaster, a secure network can help an organization:

- Ensure compliance with industry and government regulations
- Provide employees with the widest appropriate levels of access to the tools and applications they need to work remotely, as well as appropriate defenses against inappropriate use or unauthorized access
- Promote collaboration by allowing non-employees to access your network with appropriate controls
- Enhance the customer's experience
- Reduce the risk of litigation from loss of data or security breaches
- Adapt more quickly and confidently to changing business conditions
- Provide the best posture to adapt to new threat remediation requirements

How does software fit in?

At Cisco, we recommend adhering to industry leading practices to improve the security of all network components, including software. The integrity and validity of your network software is integral, as attackers can insert malicious code into a software image anywhere along the supply chain. This attack scenario could occur to any software running on any device.

Network administrators need to refer to and use recommended practices that can reduce the risk of malicious code on Cisco IOS devices. For example, they should develop and consistently apply a secure methodology for Cisco IOS software image management from the time an image is downloaded from Cisco.com until a Cisco IOS device begins to use it.

Several other recommended steps can help mitigate the risks of introducing malicious code into the network:

- Change control substantiates that changes made to network devices are requested, approved, implemented, and audited while helping ensure that only authorized and unaltered Cisco IOS software is used in the network.
- Implementing Authentication, Authorization, and Accounting (AAA) helps ensure the security of interactive access to network devices.
- Controlling access helps ensure that only the right people have the appropriate levels of access to perform necessary management functions on a network device.

Maintaining a secure repository for the software and configuration files used by the networking devices is often overlooked. Comparing the 128-bit checksum is a simple and effective way to ensure that a software image has not been altered or corrupted, in addition to ensuring the image is authentic. And configuration file backups and change control ensure that your networking device configurations are stored in a secure location. Lastly, networking devices should send log messages related to configuration changes to a secure syslog server.

Access to the secure repository should be strictly limited to those who need it and audited regularly. It is essential that the server on which the repository is stored itself be properly maintained and patched. Secure shell access, secure copy, and SNMPv3 should be used in place of telnet, ftp, and rsh/rcp when transferring configuration or software files to and from the secure server. Many steps listed here are accomplished by commercial network management tools including CiscoWorks.

Additional information for verifying Cisco IOS software images is available on Cisco.com at Cisco IOS Image Verification. And at the Cisco Security Center, you can also find reasonable practices for hardening Cisco IOS; gather free early-warning intelligence and threat and vulnerability analyses; and stay up to date with security alerts, threat activity, and PSIRT advisories from your own desktop.

Commitment for a secured network

At Cisco, we make critical security upgrades for our network OS software freely available to our customers. We recognize that you know your business better than we do, and we strive to know how networks work. We're committed to helping those who reach out to us for upgrade assistance, as together we can determine the best upgrade path for each unique network environment. (Start with your Cisco reseller or account manager to facilitate the process.)

The other thing to know is that we are working internally to harden the operating system that runs our networking products. This isn't promoted in a press release, announced in a security advisory, or touted as a new feature: it is an ongoing effort whose benefits are included in newer releases. Though we've made great strides in hardening Cisco IOS, we're continuing to do what we can to improve the resilience of our networking products. However, if you don't upgrade, all our work may be for naught. Keeping networks as secure as possible is our combined responsibility. And in turn, our efforts should have a compounding effect toward a more secure Internet.

Even with our help, the reality for you is that network upgrading takes time and, often, investment. Network devices are not all created equal, and different parts of your network have different priorities. Like many others in Cisco, I recognize the challenges in upgrading. We keep improving our platforms to reduce the resource and operational impacts caused by ongoing maintenance and upgrades. IT and security professionals must thoroughly assess risk and impact on the business to help decision makers understand the genuine threats they face by not allocating sufficient resources to update the network. Regular assessments can help you ensure that your network security keeps pace with your evolving business requirements. In this, we are really no different than other OS and hardware combinations in organizations.

Keep in mind that upgrading isn't just a one-time duty. What would happen if you suddenly had to upgrade your network due to an unforeseen disruption? The good news is that network upgrades can and must be researched, scheduled, and rigorously tested to help dramatically reduce downtime and surprises. Establishing sound design practices at the outset can help to avoid single points of failure in the network, hosts, and applications, which can make upgrading much easier than when there is a dire need to do so to avoid downtime. If mitigating risk to the business is the primary goal for IT security, then it surely makes sense for security officers to pay equal, and at times full attention to what might be the most important security upgrade of all—to the network itself. After all, we're all connected.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**