riskrecon

mastercard

Weaving a Safer Web

The State & Significance of TLS 1.2 Support

22%
of firms have not fully implemented TLS 1.2

70%
higher security findings in firms that don't fully support TLS 1.2

67%
of servers running older TLS versions also struggle to patch software

Analysis conducted by

119 Cyentia INSTITUTE

Communicating securely on the web is fundamental to the operation of the Internet. Various TLS (previously SSL) protocols deploy an apparatus of interlocking cryptographic algorithms, kept in check by a widespread network of certificate authorities to ensure the little green lock at the top of our browser helps us feel safe.

Because TLS is the conduit through which a great deal of juicy personal and financial information flows on the internet, it has long been a target of security researchers. These whitehat crypto-nerds have uncovered a menagerie of sinister-sounding vulnerabilities across multiple TLS versions, which are often decried as harbingers of Armageddon on the Internet. Perhaps this is why TLS exploits have long held the crown for "protocol most likely to have a branded vulnerability."

All this protocol breaking and refining has brought us to the current state of the affairs wherein the Internet Engineering Task Force, the National Institute for Standards and Technology, and the Payment Card Industry Security Standards Council are mandating that operators of web servers migrate to using TLS 1.2 in 2020. Additionally, TLS 1.0 and 1.1 have been (or are in the process of being) deprecated in one way or another by major browsers. This means visitors will have to navigate around cryptic browser warnings in the very near future if your website doesn't support TLS 1.2. Definitely not a good look.

In this report, we'll zoom in on the state of TLS 1.2 implementation across the Internet. We'll leverage RiskRecon's unique scan data on millions of web servers around the world to see where the rollout of TLS 1.2 is going smoothly and where it is meeting resistance. Additionally, we'll show that not supporting TLS 1.2 isn't just bad for the customers visiting unsupported websites, but can be an indicator of other security problems within an organization.

> The big takeaway is that if firms can't implement TLS 1.2 comprehensively, then they likely have bigger security holes in their network.

[2] POODLE, BEAST, Logjam, DROWN, FREAK…hackers love getting creative with their acronyms.

Current Landscape of TLS 1.2 Support

The most obvious question to ask about the rollout of TLS 1.2 is "What percentage of web servers don't yet support TLS 1.2?" We analyzed a sample of 5.5 million web servers scanned by RiskRecon and came to a heartening result: Only 2.2% of hosts that had HTTPS running did not support TLS 1.2. This is somewhat expected based on the looming browser compatibility deadline and the ease with which modern web servers can be configured to communicate with the correct protocols. It also approximately matches others who have studied the same question.[2]

Given that promising 2.2% number, we might conclude "Hey! TLS 1.2 support is something organizations as a whole are doing well. The system works". Let's pump the brakes a bit. RiskRecon not only collects data on individual hosts but is able to determine what organizations control those hosts. This allows us to ask a perhaps more pertinent question, "What percentage of organizations have not yet fully rolled out TLS 1.2 across their web infrastructure?" The answer is a less heartening 22.2%, and in fact varies quite a bit across industry. Figure 1 has those details.

FIGURE 1: PERCENTAGE OF FIRMS IN EACH INDUSTRY WITH TLS 1.2 INCOMPATIBILITIES

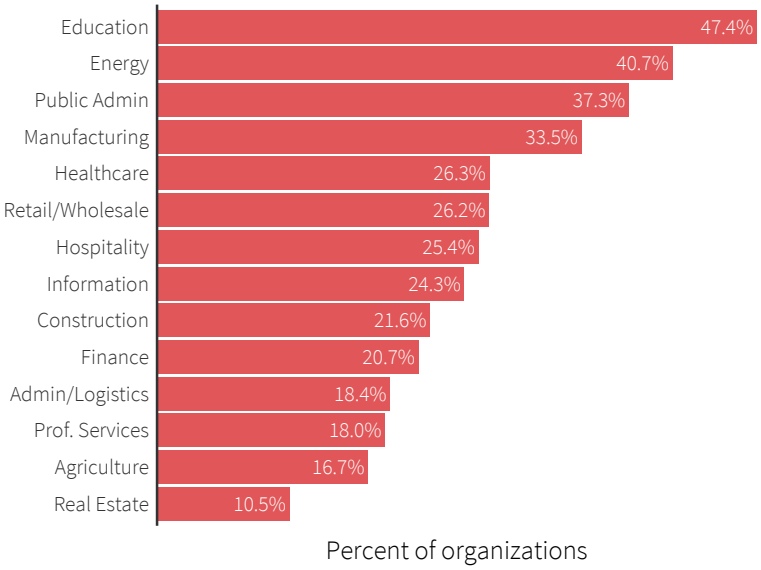


Figure 1 shows the percentage of organizations in each sector that have not yet fully implemented TLS 1.2 across their web infrastructure. The differences are quite dramatic and suggest various business and culture pressures shaping adoption.

Since educational institutions are prone to large Balkanized networks, it's unsurprising that such a high percentage haven't implemented secure TLS protocols across the board. But are these hosts collecting and transmitting important information using vulnerable protocols? I'm glad you asked, because RiskRecon also determines web host value by examining whether a website collects and transmits important PII or credential information. If we restrict our view to just these high value hosts we can zero in on where the lack of TLS 1.2 represents a substantial risk: 1 in 10 organizations transmit private information over flawed protocols.

> 1 in 10 organizations transmit private information over flawed protocols.

[3] See https://www.ssllabs.com/ssl-pulse/

Support in External vs. Internal Hosts

The next aspect of the TLS 1.2 roll-out that bears examination is whether the location of the server improves the odds of using up-to-date protocols. Specifically, whether on premises or cloud hosts are better at ensuring communication is happening securely. First let's look at our 1.6% number in comparison with hosting location.

FIGURE 2: TLS 1.2 INCOMPATIBILITY RATES AMONG EXTERNAL AND INTERNAL HOSTS

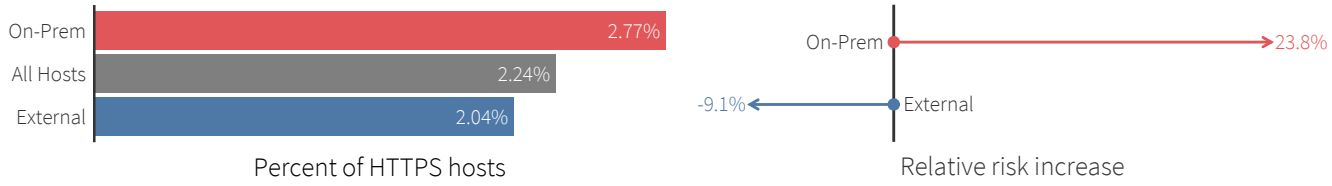
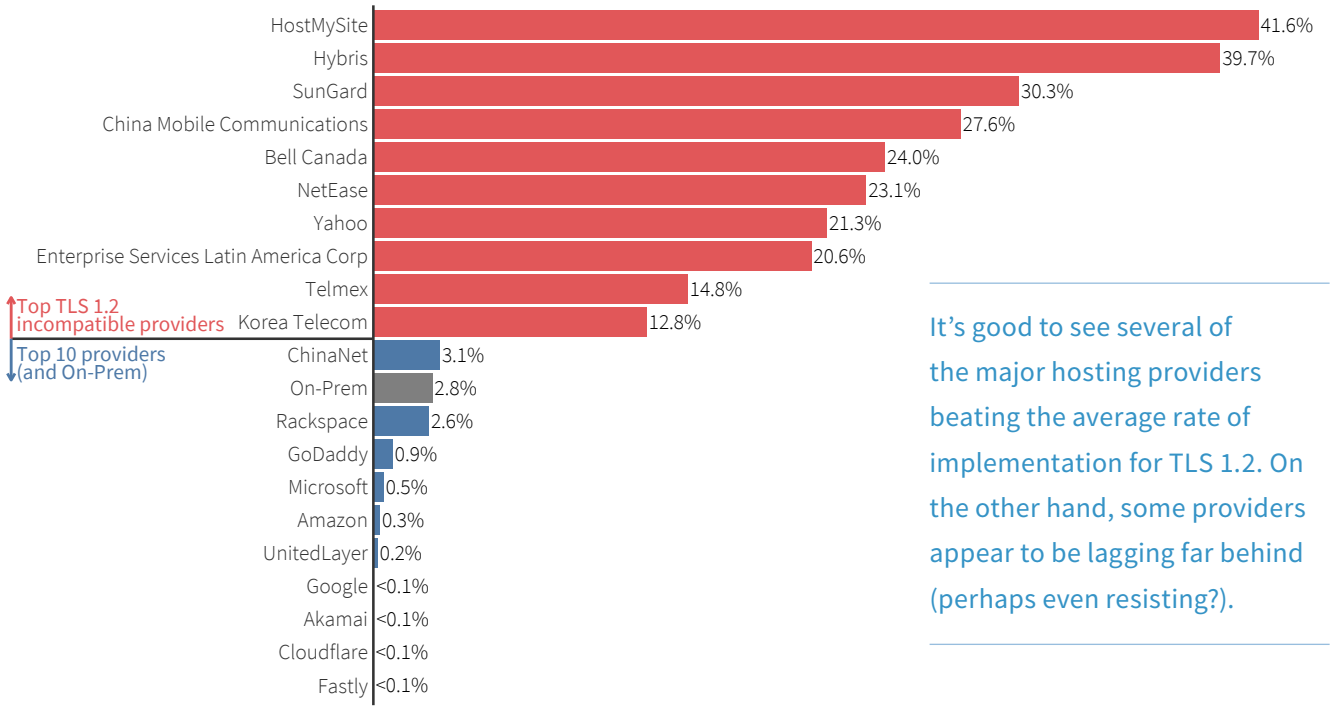


Figure 2 shows that the overall percentage of HTTPS hosts failing to support TLS 1.2 remains small when we break out on-prem and external hosts. However, when looking at various risk factors, we'd like to know how the risk increases relative to the baseline prevalence.[3] Compared to the entire population of web servers, an on-premise host is much more likely (23.8%) to fail to implement TLS 1.2 properly. Externally-hosted servers, by comparison, see a modest 9.1% decrease.

"External" is not terribly specific given the myriad of extant hosting providers. Certainly, some are doing a better job with the TLS 1.2 rollout than others. To test that, Figure 3 contrasts the top 10 hosting providers based on number of hosts and the 10 providers with the worst TLS 1.2 implementation rates. The results are stark, to say the least.

FIGURE 3: TLS 1.2 INCOMPATIBILITY RATES AMONG HOSTING PROVIDERS



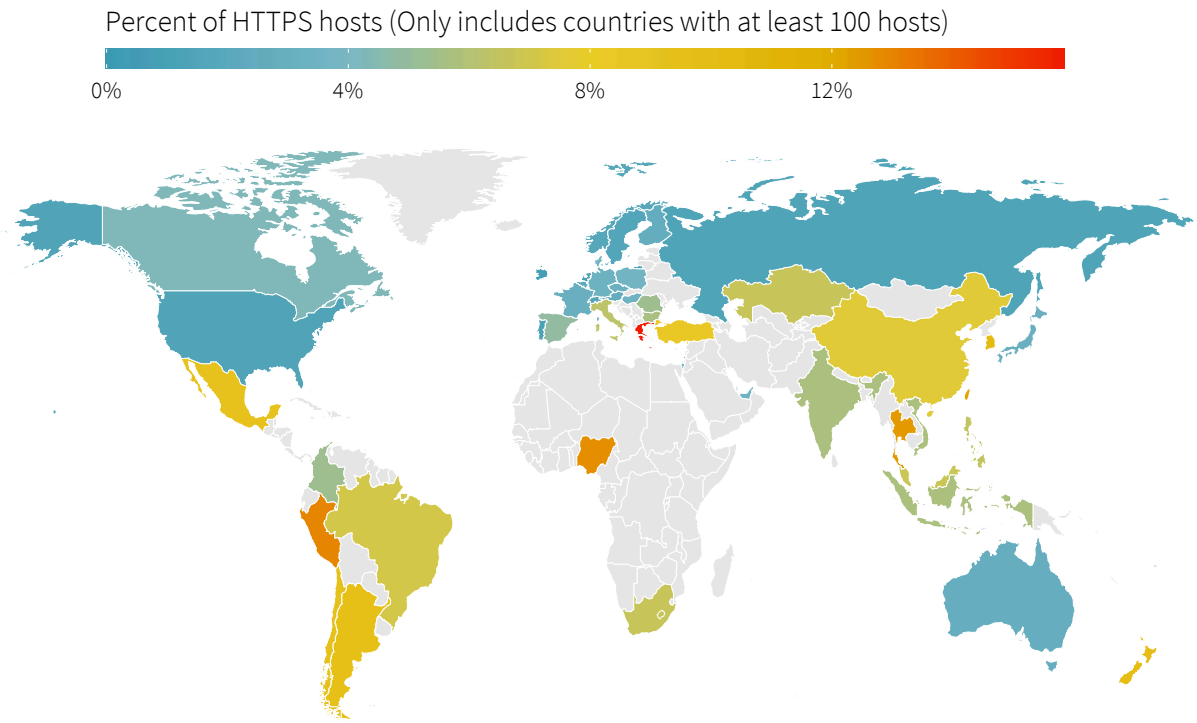
It's good to see several of the major hosting providers beating the average rate of implementation for TLS 1.2. On the other hand, some providers appear to be lagging far behind (perhaps even resisting?).

[3] We're using "risk" here according to the definition in Porta M, ed. (2014). Dictionary of Epidemiology (6th ed.). Oxford University Press. pp. 245, 252

We find it encouraging that the 10 biggest hosting providers land at the bottom of Figure 3 with impressively low rates of TLS 1.2 incompatibility. The three big clouds of Amazon Web Services, Microsoft Azure, and Google each show less than 1/5th the percentage of noncompliant hosts as those on internal networks. We'll soon see that this is a good indicator those big providers are doing things right in other security areas too.

But what really jumps out from Figure 3 is the prominence of Chinese hosting providers (China Mobile, NetEase, ChinaNet) among those lagging behind in the rollout of TLS 1.2. This may not be incompetence but rather a deliberate attempt to force the use of weaker encryption methods for the purposes of government eavesdropping. While China doesn't specifically ban the use of TLS,[4] it does have a complicated relationship with surveillance, ISP control, and encryption.[5] If we look at TLS 1.2 rollout by country in Figure 4, we see that China has one of the highest incompatibility rates. About 6.8% of servers in that country use older versions of TLS compared to the global value of 1.6%.

FIGURE 4: TLS 1.2 INCOMPATIBILITY RATES AMONG COUNTRIES



> If we look at TLS rollout by country, we see that China has one of the highest rates of servers lacking TLS 1.2 –about 6.8% compared to the global value of 1.6%.
>
> .

[4] See https://www.dezshira.com/library/legal/cyber-security-law-china-8013.html
[5] See https://www.thesslstore.com/blog/https-google-china/
[6] See Adrian, David, et al. "Imperfect forward secrecy: How Diffie-Hellman fails in practice." Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015. and Adrian, David, et al. "Imperfect forward secrecy: How Diffie-Hellman fails in practice." Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015. Both these articles indicate the need for "nation-state level resources" to successfully attack specific flaws in some TLS protocols.

TLS 1.2 Incompatibility as a Portent of Other Problems

Many TLS weaknesses are difficult for actors to exploit,[6] and most software makes it relatively easy to enable the latest protocols for communication. Running the most up-to-date cipher suite should then be an easy win for most security teams. If an organization can't pick off this low hanging fruit, are they more likely to struggle elsewhere too? Let's check and see.

FIGURE 5A: TLS 1.2 AS AN INDICATOR OF SECURITY FINDINGS

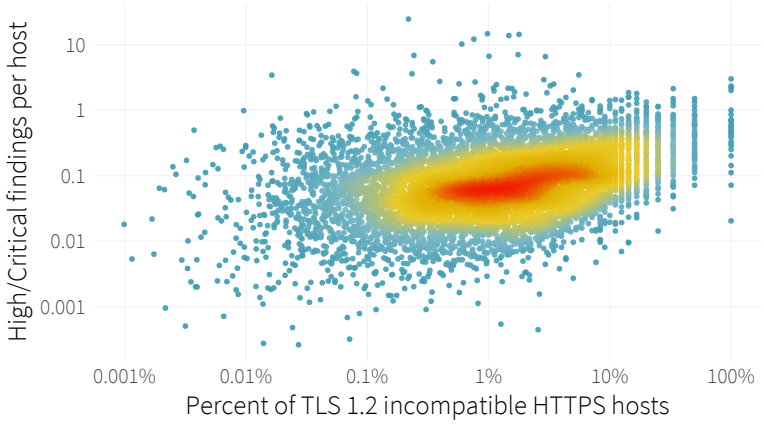
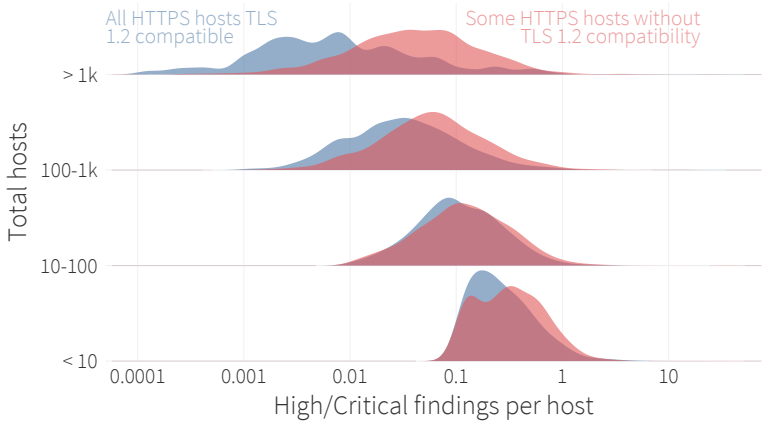


FIGURE 5B: TLS 1.2 AS AN INDICATOR OF SECURITY FINDINGS



We started with a simple correlation of TLS 1.2 incompatibility with the rate of high or critical security findings for each orgnization. The result is captured in Figure 5a, and despite a high variability, the overall pattern is pretty clear. The density of severe security findings per host increases along with the percentage of servers running older versions of TLS. The takeaway is that if firms can't implement TLS 1.2 comprehensively, then they likely have bigger security holes in their network.

Perhaps even more interesting is that declaration carries more weight for organizations with larger networks. Figure 5b compares the density of security findings between organizations with 100% TLS 1.2 implementation across all hosts (blue) and organizations with less than full compatibility (red). The increasing separation between the blue and red mounds suggests that TLS 1.2 implementation becomes an even better indicator of broader security woes in larger firms.

Overall, having any TLS 1.2 incompatible hosts increases an organization's high/critical finding density by 70%. As always, we caution that correlation is not causation. Fixing your TLS implementation will not magically make other security problems go away.

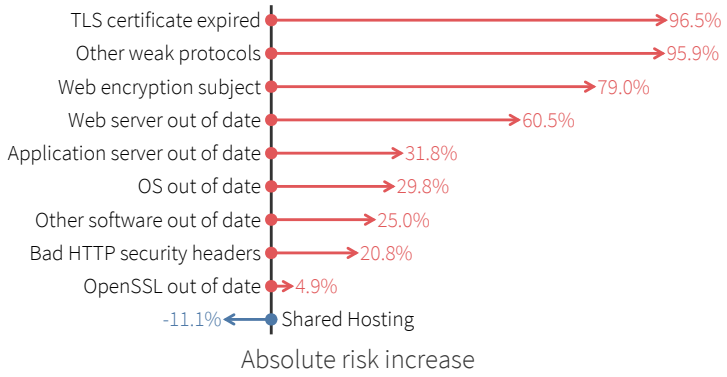
> The takeaway is that if firms can't implement TLS 1.2 comprehensively, then they likely have bigger security holes in their network.

[7] Both practically and statistically significant. Figure 5a indicates a statistically significant ($p < 0.001$) Spearman's rho of 0.39 and Figure 5b shows a statistically significant ($p < 0.001$) impact of TLS 1.2 incompatibility on the density of high/critical findings in a linear model, controlling for the number of hosts in an organization.

But what exactly are those problems that often co-occur with TLS 1.2 incompatibility? To find out, we profiled high and critical security findings in servers running older versions of TLS. Some expected and unexpected results show up in Figure 6.

First the expected results: Figure 6a reveals hosts that don't implement TLS 1.2 also tend to have other web application findings related to expired certs, bad headers, etc. Somewhat more interesting is that these hosts appear to make a habit of running out of date software. And not just web server software, but also things as fundamental as out of date operating systems and content management software.

FIGURE 6A: FINDINGS CORRELATED WITH TLS 1.2 INCOMPATIBILITY



Read Figure 6a and 6b like "96.5% of hosts that don't fully implement TLS 1.2 also exhibit '*TLS certificate expired*' findings."

FIGURE 6B: FINDINGS CORRELATED WITH TLS 1.2 INCOMPATIBILITY

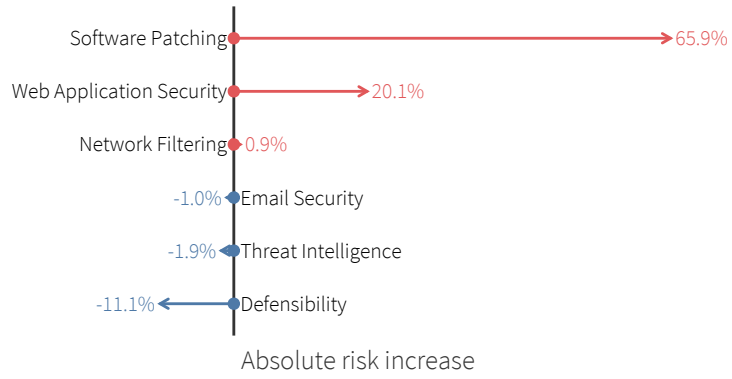


Figure 6b zooms the view to a higher level categorization of findings. In many ways, this tells a similar story to that of 6a. But the wider scope presented here is potentially a stronger indictment. Nearly two-thirds of servers using older versions of TLS also show evidence of poor software patching. Where there's smoke...

All of this gives strong credence to the concept of using simple "cyber hygiene" tests like this as an overall indicator of risk management capabilities. It also reinforces the classic adage that good cybersecurity is a function of IT done really well.

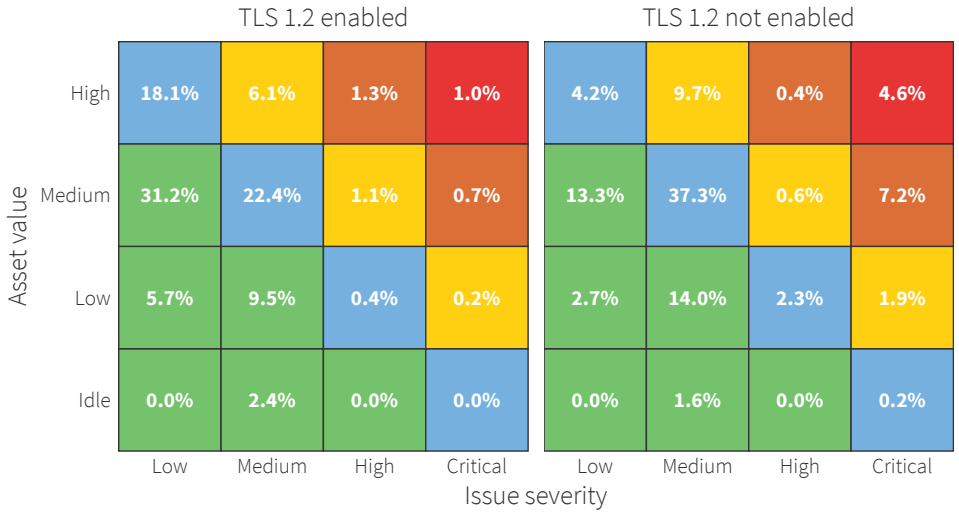
"This gives strong credence to the concept of using simple "cyber hygiene" tests like this as an overall indicator of risk management capabilities. It also reinforces the classic adage that good cybersecurity is a function of IT done really well.

Conclusions

The ability to securely communicate with the outside world through an organization's website is a fundamental demonstration of security competency. As we delved into TLS 1.2 adoption, we uncovered interesting nuggets about who's doing it well, who's not, and how a firm's handling of web encryption can be an indicator of other problems in their network.

We leave you with one final figure presenting a view of this topic through the lens of RiskRecon's risk matrices. The upper right is where your eye should be drawn. Assets rated as high value support sensitive and/or critical business functions. That's why the 5x jump in critical security issues among high-value servers running older TLS versions is a red flag.

FIGURE 7: ISSUE RISK MATRICES FOR SERVERS WITH TLS 1.2 ENABLED VS. NOT ENABLED



Assets rated as high value support sensitive and/or critical functions. That's why the 5x jump in critical security issues among high-value servers running older TLS versions is a red flag.