NUMBER 62 | JANUARY 2022

NTT DATA
Trusted Global Innovator

# Radar

## Cybersecurity magazine

# CYBERSECURITY AND INNOVATION AFTER DISRUPTION

We start 2022 with the belief that we will never go back to business as usual. We have lived through a major disruption. What major innovative technology trends will we experience from this point onwards?

Our organisations will evolve along with trends that challenge the way we see the world. A few months ago, the word “metaverse” entered our everyday vocabulary. The metaverse, a metaphor for the entire digital universe, where geo-positioned content enriches our real universe by offering a world of services that we can access through applications and digital devices, such as a mobile phone or virtual reality glasses.

Another trend that is coming is generative AI, at a time when there is still a feeling that AI is not yet 100% embraced.  Generative AI will allow us to create from scratch, giving algorithms new autonomy.

In a world where talent is becoming a challenge, hyper-automation is emerging as a trend ready to close a number of gaps: human error, efficiency, and labour shortages.

And in our favourite world, the world of cybersecurity, discussion of the cybersecurity mesh has begun, as a flexible architecture that helps to establish perimeters around people and systems, with security measures and controls in place to further enhance its protection.

And although we are part of a specific trend, from the security areas we are now defining how to protect the rest of the trends. How to build around the metaverse in a secure and respectful way with people’s information. How the algorithms created by artificial intelligence itself are robust and secure. How automation is done in a secure way and, in this case, how cybersecurity itself is automated.

With all these trends in perspective, we at NTT DATA Europe and Latin America wish you an excellent 2022!

**Enrique Bernao Rosado**
Cybersecurity Manager at NTT Data Spain

# CYBER NEWS

The Christmas and New Year's festivities are special dates where companies and individuals have large amounts of money available to celebrate during these days, not to mention that there is a bit of distraction due to holidays and the motivation to take advantage of possible discounts or gifts that could be received.

All this opens the door to cyber-criminals who are always waiting to take advantage of the best opportunities to try to carry out fraud, phishing attacks, vishing, or identity theft, among others.

While many of us know to be wary of emails, text messages that surprise us with gifts, discounts, congratulatory messages, account problems and more, there are still people who are unaware of the hidden dangers that affect the cybersecurity and economy of individuals and businesses.

> "Fraud during the 2021 Christmas season culd exceed 53 million dollars".

With the above in mind, with this cyber-chronicle we want to tell you some of the most important cybersecurity news at this time of year and of which any of us could become a victim, in addition to being able to keep up to date with the latest techniques and strategies used by attackers to breach our security.

Among the highlighted news of recent days, we have the phishing attack suffered by the decentralised lending protocol bZx, which resulted in losses of more than $55 million dollars. It was discovered that a cyber-criminal using phishing gained access to the PC of one of the bZx developers, which resulted in the theft of this person's private keys. This event was revealed on November 5th by bZx itself, and after deceiving the employee, the attacker left the developer's wallet empty and stole the Polygon and Binance Smart Chain (BSC) implementation keys of the bZx protocol; as a bonus for our ethical hacking friends, Polygon paid Gerhard Wagner a reward of approximately $2 million dollars for a critical vulnerability found.

On the other hand, according to the FBI, fraud during the 2021 Christmas season could exceed 53 million dollars, a figure obtained during Christmas 2020.

The FBI says that because of the pandemic and the increase in the number of people surfing the internet, cyber-fraud, and attacks by cyber-criminals, who take advantage of some people's lack of awareness to steal their credentials and bank details, continue to grow exponentially. To do this they use emails, fraudulent websites, and text messages that, after being used by the victims, end up giving sensitive information to the attackers. We must be careful!

It is not always the end users who are to blame. It is also important to mention configuration errors in the infrastructures of large companies, for example, security researchers found a misconfigured database in the cloud that leaked approximately 300,000 logs with sensitive and personal information of e-commerce users.

After an investigation, Safety Detectives found the Elasticsearch database in the cloud and discovered that this database had been exposed without any protection since November 2020.

However, the detected data leaks date back to 25 July this year and the leaked logs contain information such as names, phone numbers, emails, home, and delivery addresses.

Now tackling a slightly different topic and mentioning the way cyber-criminals do business with ransomware, which is sold or leased on the dark web; Digital Shadows has discovered that now these cyber-criminals have started leasing zero-day vulnerabilities on the dark web, which are said to be bought by other criminals, commanding prices as high as $10 million according to Digital Shadow.

But it's not all bad news, it should also be mentioned that Microsoft has fixed XSS reflected in Exchange Server; researchers from Vimeo detected the vulnerability registered as CVE-2021-41349 that allowed reflected Cross Site Scripting attacks, a vulnerability that allows multiple attacks such as phishing, application status changes, sending emails, among others. Since this vulnerability is of medium criticality due to its low attack complexity, Microsoft immediately set about the task of remediating it by generating patches for Exchange Server 2013, 2016 and 2019. You can see the PoC here.

We close this cybernews in the midst of intense work on the remediation of the Log4j vulnerability, which has come to revolutionise our work in December. Different media have already published how to mitigate it. We will talk more about it in our next edition.

# CURRENT AND FUTURE CHALLENGES FOR CISOS

**By: NTT DATA Spain**

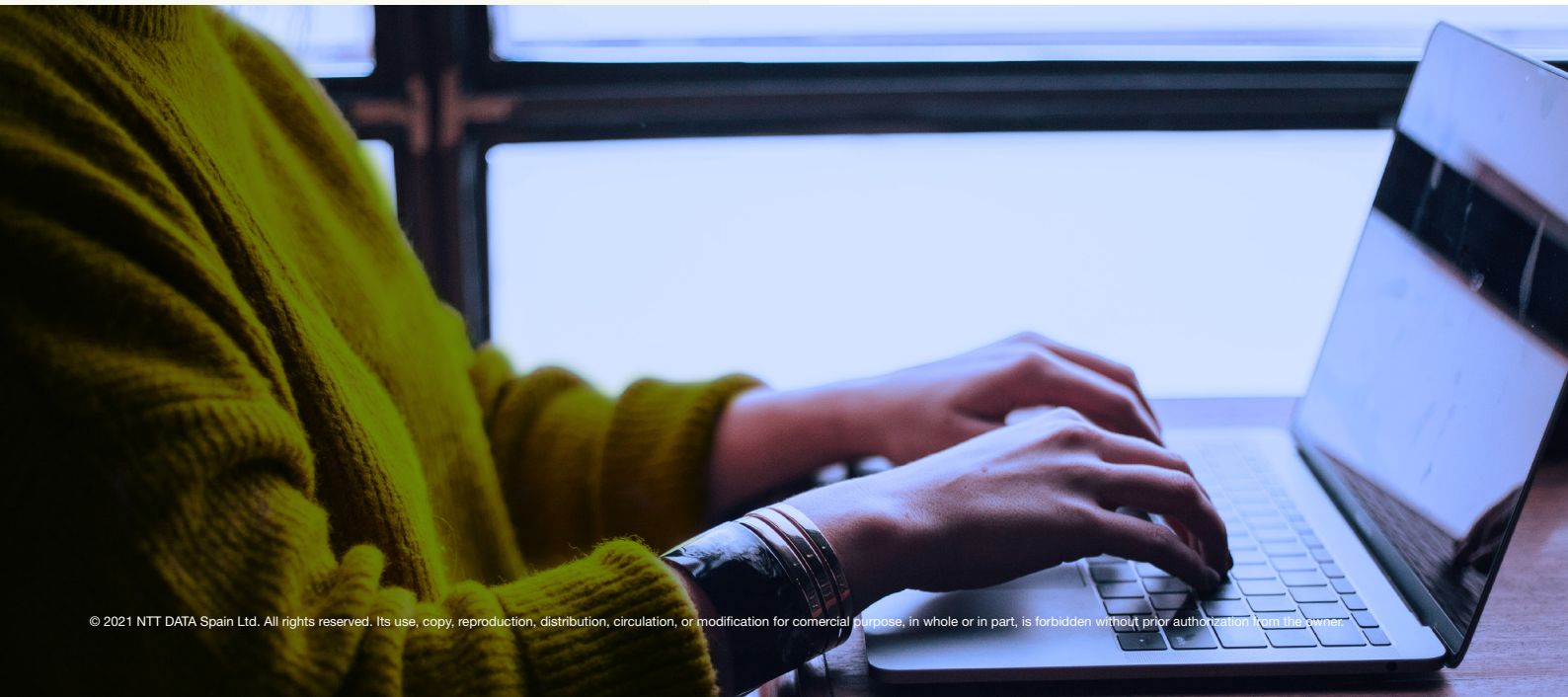
**As organisations have sped up their digital transformation in the wake of all the global changes we are experiencing, CISOs have become a key part of the business infrastructure. CISOs are at the frontline of the various threats posed by this change, by the new technologies that have been necessary to adopt. Their main objective is to ensure that companies can protect themselves from cyber-attacks.**

However, despite the measures being taken to address new threats, it remains a constant challenge for companies to control their security risks, mainly for two reasons.

- On the one hand, attackers are continuously adapting their tactics to breach systems, and these are becoming increasingly sophisticated.
- On the other hand, the vision of CISOs and security departments remains tool-based, while more and more studies agree that they have to think on a business-driven basis.

Although CEOs have been seen to allow increased investment in the resources CISOs need to drive security in the digital shift, there are still challenges for security departments to overcome:

- Work overload and variability: CISOs must be knowledgeable about laws, regulations, good security practices, as well as being technical, knowing about hacking, secure development, and the cloud. They must process large volumes of information and numerous alerts from monitoring centres, as well as understand the challenges of new technologies. Only a team of differentiated and specialised profiles can meet all these knowledge needs.
- The acceleration of digital change is outpacing investment in cybersecurity: the financial allocation to cybersecurity areas still does not seem to be sufficient to really address organisations' needs.
- Communication: The CISO should focus on working towards a collaborative and inclusive culture, taking into account cybersecurity awareness. People are and will be the key to cybersecurity and proper communication helps to cut off different attack vectors that are still very effective today.
- Shortage of cybersecurity professionals: While there are professionals with knowledge in the field of cybersecurity, there is a shortage of professionals with specific skills, mainly for the new technologies needed in this great digital change (Blockchain, cloud applications, IoT).



In addition, there is increasing talk between cybersecurity and business, between security projects and alignment with the contribution of value to the company.

This alignment between cybersecurity and business is undoubtedly the common thread that CISOs should use to make decisions in the coming years.

This relationship will allow much better targeting of investments to be made, in order to focus them on the protection of the assets that give companies their true value.

To conclude this article, and as a preliminary to the next one, we would like to give a special mention to Blockchain technology, which we already talked about in our previous RADAR and which we dedicate an additional article to in this one.

Blockchain is bringing and will bring profound changes to the way the banking sector operates. Business models and ways of operating are challenging even for many of us who are involved in new technologies.

### How will this technology impact the day-to-day work of CISOs and security?

If CISOs really want to accompany the business, they must understand what new changes in their companies will come from blockchain technology, foster the security of new applications and be a lever for growth.

One of the new trends is crypto-banking. The world of cryptocurrencies is and is predicted to continue to grow over the next few years. Mastercard, for example, in February of this year announced the introduction of direct support for payments in certain cryptocurrencies, eliminating the need for conversion at the point of sale and allowing merchants to directly accept cryptocurrencies. Countries such as El Salvador have legalised bitcoin as the country's currency.

Across banking, Fintech also brings new business models that we need to protect.

What security controls do we need to apply to these new technologies? how do we make people perceive them as secure? how do we ensure the traceability of the transaction in case an incident occurs?

These answers will be resolved over time, but in the meantime, the onus is on security areas to learn and adapt.

We then include a second article on technical aspects, giving way to a technical aspect of Blockchain and an applied case.

# FIREWALL RULE AUTOMATION WITH SMART CONTRACTS

By: NTT DATA Spain

**In this article we will introduce you to a new and innovative way of dealing with some of the security issues that arise in blockchain networks. Do not get us wrong, blockchain offers security, no one can manipulate the data, but the problems that will be mentioned refer to the security "holes" that appear when nodes are exposed without security considerations.**

To achieve that purpose, it is possible to write smart contracts that keep an up-to-date status of the nodes allowed to connect and use that information to automatically update our firewall rules in near real time.

The approach to guide you on this path will go from the specific to the general. First we will show you the most basic implementation to automate firewall rules through smart contracts on a single node. Finally, you will have a general approach on how to approach security at the management level (cloud/on-premises providers). This approach is not intended to replace the current schemes used by organisations to secure their environments but is a contribution to improve security by leveraging the trust offered by blockchain networks.

Although everything mentioned so far is an almost general concept, we will exemplify the automation of firewall rules through smart contracts written in Ethereum; we will also explain an intermediate component between the Ethereum network and the firewall rules.

## Permissioned networks in Ethereum

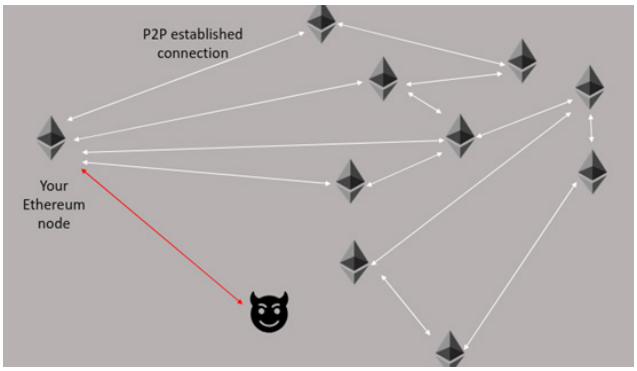
We are going to delimit our journey by focusing on Ethereum networks. Permission networks add a layer of security at the application level. It allows you to control who can join the network.

Ethereum client implementations such as Parity and Hyperledger Besu have two ways to create a permissioned network.

1. Using files on each node to specify which other nodes can communicate with that node.
2. Another interesting approach to achieve the same purpose is the use of smart contracts. This implementation is known as onchain permissioning. Basically, in this approach all nodes that obey the permissioning smart contract form an authorised network. The contract decides which nodes to connect to. It is worth saying that this approach is more dynamic; as soon as the list of nodes is updated in the smart contract, the nodes start accepting the new permissioned node.

## Pain points

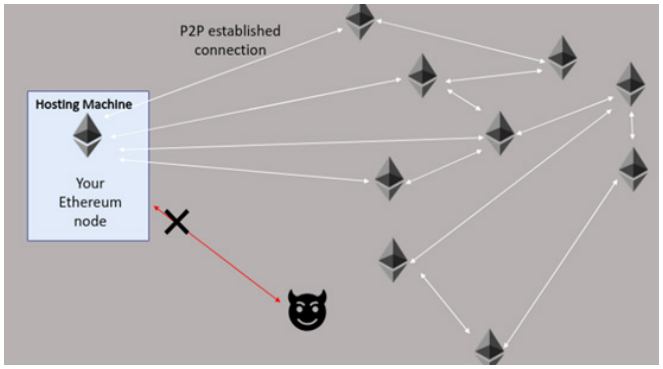
Analysis of current permissioned networks shows that nodes are accessible at the application level, so any other node, even if it is not in the smart contract, can reach the P2P node's ports and try to attack it. Even when the node does not accept connections other than those logged in the smart contract, bad actors can still perform spam attacks on the exposed P2P ports.



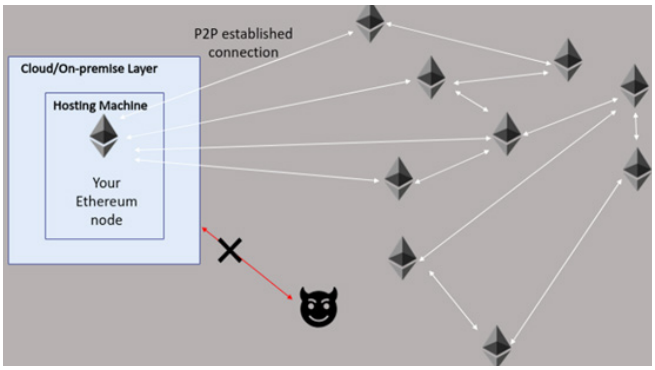

To protect access to our nodes we can choose to use firewall rules. This approach adds a layer of security so that only authorised nodes can reach our Ethereum nodes.

Firewall rules can be applied on:

- The hosting machine where the node lives




- Cloud/On-premises infrastructure




Firewall rules add more security, but also more complexity to our configuration, as they have to be updated manually.

Controlling Firewall rules manually may cause synchronisation to be lost in some consensus protocols, e.g., IBFT2.0 requires a minimum number of active validators (>=2/3 of the validators in the list) in order to keep adding blocks. Communication between these validators must be guaranteed. In this case, if new validators are added to the network and the firewall rules of other validators have not been updated to allow connection to the new validators, the network could stop due to a communication failure between the validators.

## Analysis

It is our view that having networks with permissions is not enough in terms of security. On the other hand, using firewall rules manually has its own problems.

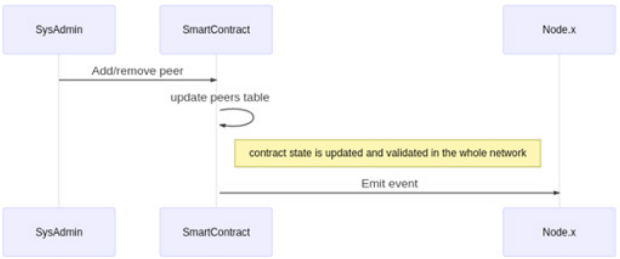
Nodes should have a way to protect themselves from a variety of attacks that could be performed when malicious actors reach our nodes through security holes. It might be useful to have a dynamic way of handling firewall rules.

## Onchain Firewall Rules

So far we have analysed permissioned networks and firewall rules. In this section we are going to show how to use permissioning smart contracts to increase security at the system administrator level to guarantee Ethereum service relief and increase protection to our node. To achieve this purpose, it is possible to automate firewall rules through smart contracts and in this scenario nodes can use the smart contract as a source of trust when modifying rules. In the following section we are going to apply smart contracts (through emitted events) to automatically update the firewall rules.

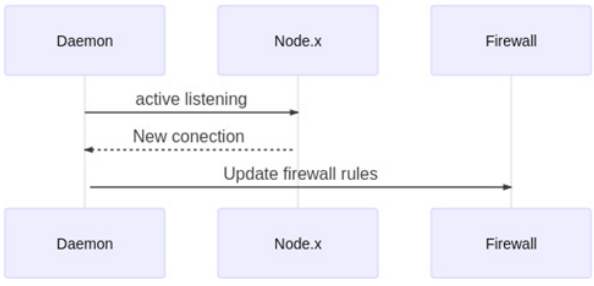
## Implementation

The following diagram shows how network administrators

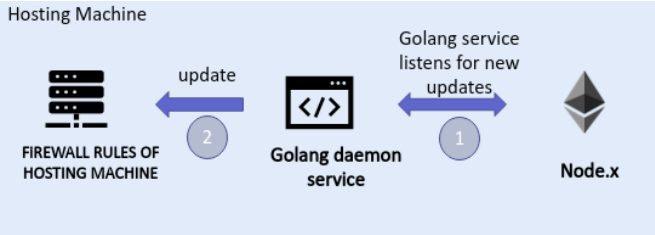



with permissions can update the nodes allowed to join a network.

- The Node.x can be your node that is used to interact with the network.
- In the following diagram you can see a daemon service that is listening for the smart permissions contract through your Node.x. Once the daemon realises that a new event has been issued, it updates the firewall rules.

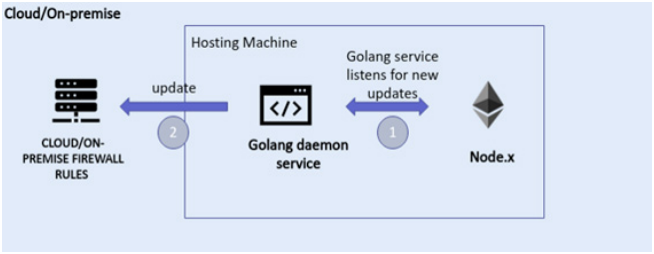


Up to this point we have seen general diagrams, now let's check a particular implementation. In this diagram the daemon service is notified by events issued by the smart permissions contract. As soon as those events arrive the daemon service updates the firewall rules on the hosting machine where the Node.x lives. If you are curious about how this particular implementation has been implemented, find the code here.




The above diagram can be extended. For example, instead of updating only the Firewall rules on the local hosting machine, the daemon service can update the cloud/on-premises Firewall rules directly.

This way you make sure that your node is connected to trusted nodes in the network. Any malicious actor will not be able to reach your Ethereum nodes because the nodes are protected at a higher level.




## Conclusion

One of the main characteristics of blockchain technologies is trust. In this article we have shown how it is possible to automate firewall rules by leveraging blockchain technologies and smart contracts as a source of trust for security.

You have also seen how we can have secured nodes and still be able to interact with other trusted nodes (other organisations).

Finally, you no longer need to worry about firewall rules because they can be automatically updated by the blockchain network.

# TRENDS

## Cybersecurity mesh as an evolution of traditional security architecture.

Like many technological axes, cybersecurity is evolving to adapt to an increasingly decentralised and autonomous time.

A new approach emerges here, the Cybersecurity Mesh approach, which seeks to ensure that every infrastructure, software, hardware, and equipment is effectively mapped and secured. This architectural approach puts every element in a network at the centre of cybersecurity by establishing a perimeter around it.

By analysing the network around each element, in combination with the functions and permissions that each element has, new security controls are defined and sought to protect this operation.

In this way, thinking in terms of a cybersecurity mesh helps organisations to protect all their assets, regardless of where they are, that is, whether they are inside the company's security perimeter or outside it.

Benefits of mesh implantation:

- It places identity management as a key point of entry to all assets in the mesh, whether people, platforms, or systems, and allows access to be redesigned from a more flexible but more robust point of view.
- It encourages the inclusion of security controls that protect the day-to-day operations of a person or system. The mesh is visualised as a flexible but well-protected system.
- It can be combined with other disruptive technologies such as blockchain in case critical operations need to be secured.
- It adapts well to the new, distributed and highly flexible working model.

The next step is to create robust security mesh implementation methodologies to make organisations' protection more flexible. This is an interesting path to follow in the coming months. We will closely follow its evolution in order to put it into practice.

# VULNERABILITIES



## HP

CVE-2021-39237; 39238
Date: 30/11/2021

**Description**. Two security researchers have discovered two security vulnerabilities in HP printers that have been exposed for more than eight years. By exploiting the first one, a local attacker could exploit it to reveal sensitive information, and with the second one, a remote attacker could cause a buffer overflow and execute arbitrary code.

**Link:** https://thehackernews.com/2021/11/critical-wormable-security-flaw-found.html

**Affected Products.**

- A total of 150 different models of multifunction printers are affected.

**Solution**: Apply the security patches published by the manufacturer.

## Hitachi Energy

CVE-2021-35533; 35535; 3449; 20225; 2023; 22278; 23840; 23841; 3516; 3517; 3518; 3537; 3541; CVE-2020-14308; 14309; 14310; 14311;15705; 15707; 14372; 25632; 27749; 27779; 24977; 1968; 1971; 24977; 10713; 1563, CVE-2019-1549; 1547; 20388, CVE-2017-8872
Date: 02/12/2021

**Description.** Multiple vulnerabilities of varying severities have been reported in various Hitachi Energy products. By exploiting these vulnerabilities an attacker could reboot the computer, hijack sessions, cause a denial of service condition, install malicious software or access stored information.

**Link**: https://www.cisa.gov/uscert/ics/advisories/icsa-21-336-04
https://www.cisa.gov/uscert/ics/advisories/icsa-21-336-05
https://www.cisa.gov/uscert/ics/advisories/icsa-21-336-06
https://www.cisa.gov/uscert/ics/advisories/icsa-21-336-07
https://www.cisa.gov/uscert/ics/advisories/icsa-21-336-08

**Affected Products.**

- RTU500 series CMU, all firmware versions 11, 12.0, 12.2, 12.4, 12.6, 12.7, 13.0, 13.1 and 13.2.1;
- Relion 670/650 series, all revisions of version 2.2.0;
- Relion 670/650/SAM600-IO series, all revisions of version 2.2.1;
- Relion 670 series, all revisions of version 2.2.2;;
- Relion 670 series, all revisions from version 2.2.3 to 2.2.3.3;
- Relion 670/650 series, all revisions of version 2.2.4;
- APM Edge, versions 1.0, 2.0 and 3.0;
- PCM600 Update Manager, versions 2.1, 2.1.0.4, 2.2, 2.2.0.1, 2.2.0.2, 2.2.0.23, 2.3.0.60, 2.4.20041.1 and 2.4.20119.2.

**Solution:** For RTU500 products affected by CVE-2021-35533:

- Deshabilitar la función BCI IEC 60870-5-104 si no es usada.
- Actualizar a una versión de firmware 6.5.0 o posterior.

- Update Relion products to version 2.2.5.
- Update APM Edge to version 4.0.
- Update PCM600 Update Manager to version 2.4.21218.1.

For RTU500 products affected by other vulnerabilities: update to the appropriate version as indicated in the manufacturer's advisory.

# PATCHES

## SonicWall

Date: 08-12-2021

**Description.** SonicWall has released security updates for several of its product lines. Specifically, these updates address a total of nine vulnerabilities, of which two are critical and the rest are high. Through their exploitation, an attacker could take control of an affected system or execute arbitrary code. The vulnerabilities that would allow remote code execution are due to a DLL Search Order Hijacking and buffer overflows.

**Link:** https://www.cisa.gov/uscert/ncas/current-activity/2021/12/08/sonicwall-releases-security-advisory-sma-100-series-appliances
https://www.sonicwall.com/support/product-notification/product-security-notice-sma-100-series-vulnerability-patches-q4-2021/211201154715443/
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0025
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026

**Affected Products:**

- SMA 100 Series: SMA 200, 210, 400, 410, 500v (ESX, Hyper-V, KVM, AWS, Azure);
- SonicWall Global VPN client, version 4.10.6 (32-bit and 64-bit) and prior.

**Solution**: Install the relevant updates.

## Bosch

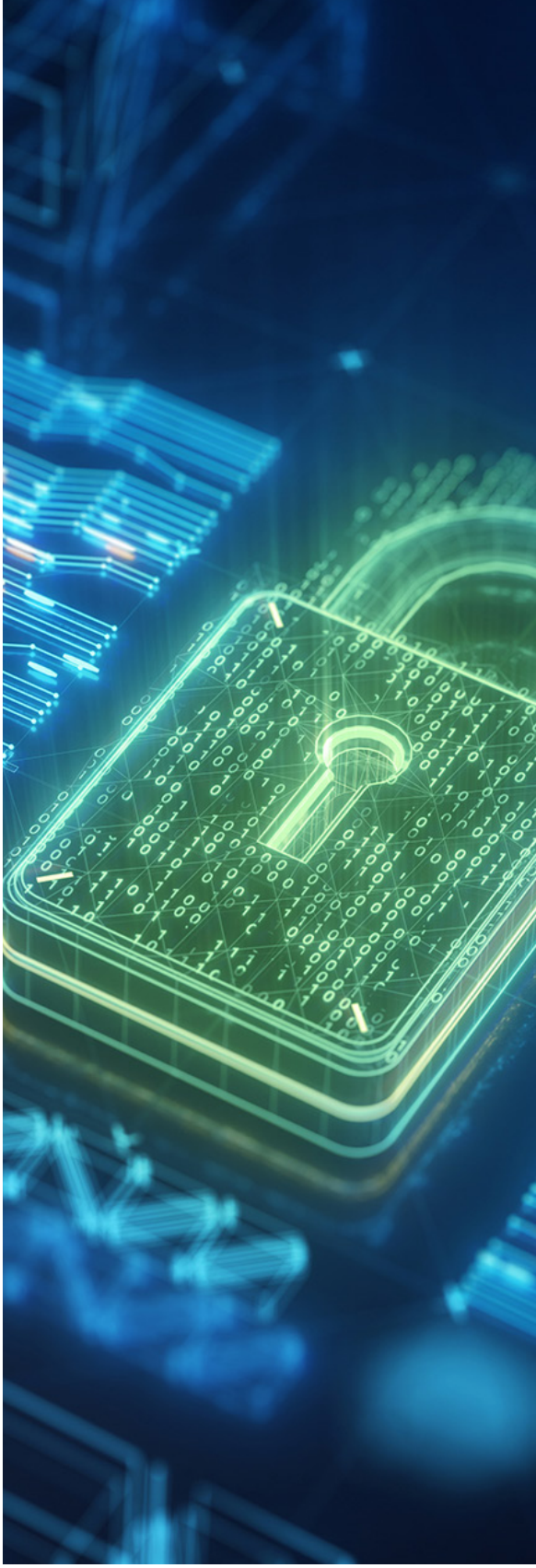
Date: 09-11-2021

**Description.** Bosch has just released several update packages in order to fix multiple vulnerabilities in several of its products. These vulnerabilities in question could allow an attacker to deny service or send unauthenticated commands on the VRM. Exploitation would occur by sending a specially crafted request that could cause a service to crash. In addition, in the case of a VRM, this denial would make it possible to send more unauthenticated commands. On the other hand, another security flaw that is addressed is the sending of a specially crafted configuration packet that could allow arbitrary commands to be executed in the context of the system.

**Link:** https://psirt.bosch.com/security-advisories/bosch-sa-043434-bt.html

**Affected Products:**
Bosch AEC, version 2.9.1.x and prior; Bosch APE, version 3.8.x.x and prior; Bosch BIS, version 4.7 and prior; Bosch BIS, version 4.8 and prior; Bosch BIS, version 4.9 and prior; Bosch BVMS, version 9.0.0 and prior; Bosch BVMS, versions between 10.0 and 10.0.2 (not included); Bosch BVMS, versions between 10.1 and 10.1.1 (not included); Bosch BVMS, versions between 11.0 and 11.0.0 (not included); Bosch DIVAR IP 7000 R2, with the configuration 'using vulnerable BVMS version; Bosch DIVAR IP all-in-one 5000, with the configuration 'using vulnerable BVMS or VRM version'; Bosch DIVAR IP all-in-one 7000, with the configuration 'using vulnerable BVMS or VRM version; Bosch VJD-7513, version 10.22.0038 and prior; Bosch VJD-8000, version 10.01.0036 and prior;Bosch VRM, version 3.81 and prior; Bosch VRM 3.82, version 3.82.0057 and prior; Bosch VRM 3.83, version 3.83.0021 and prior; Bosch VRM, versions between 4.0 y la 4.00.0070 (inclusive); Bosch VRM Exporter, versions between 2.1 and 2.10.0008 (inclusive);

**Solution:** Install the latest version of the corresponding product.



# EVENTS

## IEEE Consumer Communications & Networking Conference

**8-11 January 2022 |**

From 8-11 January, the IEEE is hosting the first conference of 2022, a gathering of researchers, developers and professionals from academia and industry working in all areas of consumer communications and networking, presenting the latest technical advances and solutions in the areas of home networking, consumer networking, enabling technologies (such as middleware) and novel applications and services. The conference includes a programme of technical sessions, special sessions, enterprise application sessions, tutorials, and demonstration sessions, and it is entirely virtual.

**Link:** https://ccnc2022.ieee-ccnc.org/

## FloCon 2022

**11 January 2022 |**

While past editions focused on network flow data, this year's Flocon will focus on improving network security through data analysis supported by various innovative technologies such as Machine Learning. It will provide an in-depth look at the latest tools, methods, and processes for using data to defend networked systems. You will also meet and connect with other attendees from different industry organisations around the world through discussions, competitions and other FloCon social events..

**Link:** https://resources.sei.cmu.edu

## Ascent: Spotlight on Cybersecurity

**12 January 2022 |**

This event, which will be held in a virtual format, will bring together the country's top cybersecurity leaders in SaaS and technology. More than 150 CISOs and senior cybersecurity leaders, with a full day of keynotes, talks, interactive panels, and networking galore.

**Link:** https://www.ascentconf.com/event/cybersecurity/

## Enterprise Data Governance Online 2022

**26 January 2022 |**

Enterprise Data Governance is a free online event, consisting of six live presentations focused on the key strategies that every data person needs to know to build or manage a successful Data Governance programme. Each session will cover topics related to Data Governance, Data Quality, Enterprise Information Management, new data-driven technologies, among others. The combined expertise of a number of leading industry professionals will be brought to the table for this purpose.

**Link:** https://www.cpdpconferences.org/

# RESOURCES

## Top 10 SANS Summits Talks of 2021

In this SANS Blog post, we can find a list of their top 10 most valued talks held in 2021. According to the opinions and evaluation of the attendees of the total of 13 events, with 275 talks by the best cybersecurity professionals from around the world, SANS shows us the most outstanding talks.

**Link:** https://www.sans.org/blog/top-sans-summits-talks-2021/

## CCMv4.0 Auditing Guidelines

We recommend the latest publication: CCMv4.0 Auditing Guidelines from the Cloud Security Alliance. As it is known, version 4 of the Cloud Control Matrix released in 2021, includes additional new components, such as the CCM v4.0 Implementation Guidelines and auditing guidelines. In this document, you will find step-by-step instructions on how to audit each CCM v4.0 control. Auditors are provided with a set of assessment guidelines for each CCMv4.0 control specification with the aim to improve the auditability of controls and help organisations to comply more efficiently with the regulation. We invite you to take a look at this report and the latest news from the CSA.

**Link:** https://cloudsecurityalliance.org/artifacts/ccm-v4-0-auditing-guidelines/

## Day 1 Summary – XV STIC CCN-CERT Conference: Ransomware, Cyber-Intelligence and Digital Society

From Cybersecurity News they tell us the summary of day 1 of the: XV STIC CCN-CERT Conference, this event is one of the most important meetings in terms of cybersecurity. The summary covers the topics exposed in Cyber-Intelligence and National Network of Cybersecurity Operations Centres, Crisis Management, Digital Transformation, among others.

**Link:** https://cybersecuritynews.es/

## Secure e-Commerce

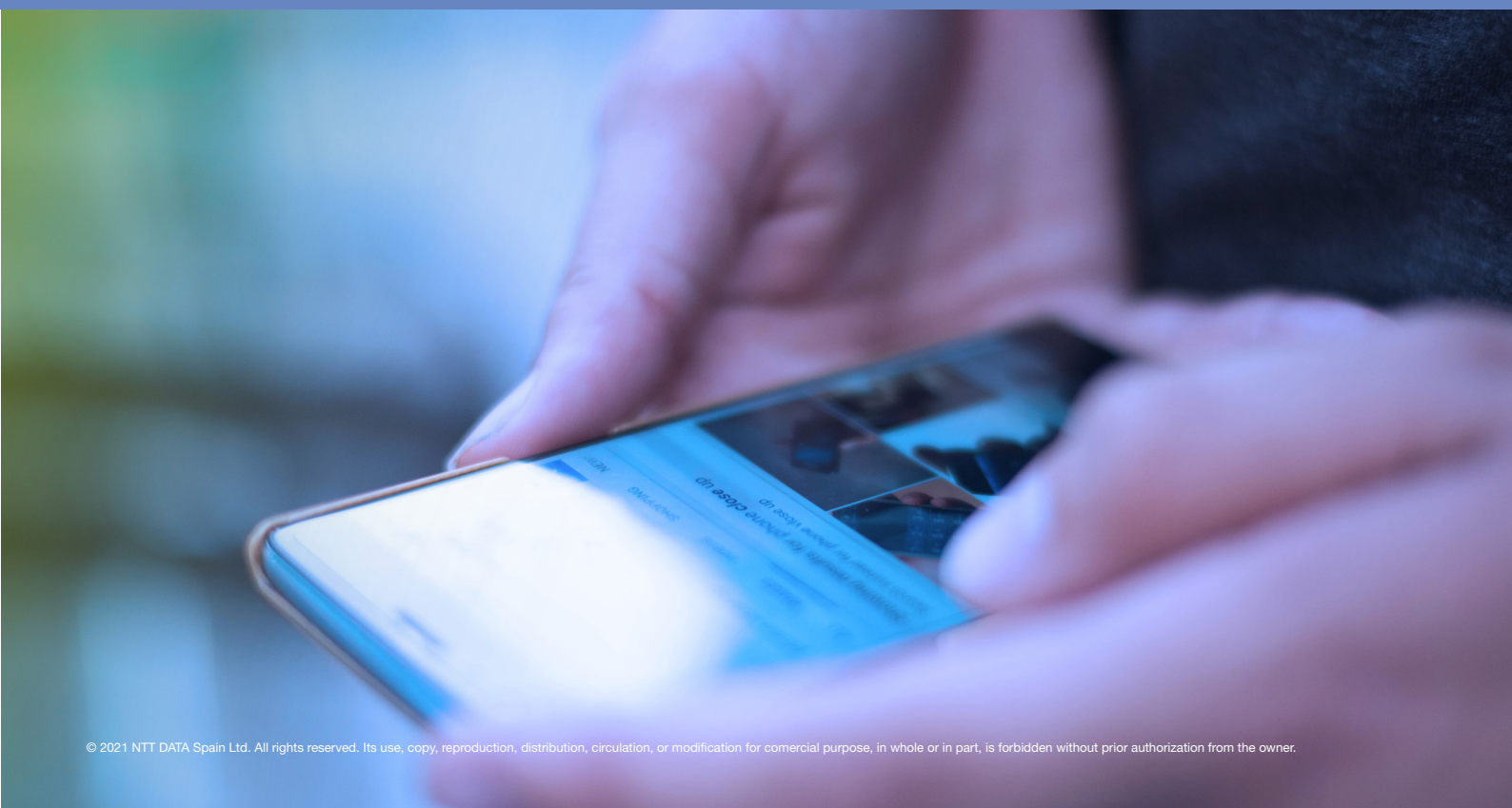
Incibe brings us a new topic in its blog to present the main security recommendations, as well as the advantages and problems that a company that has or wants to make use of e-commerce to offer its products or services over the Internet may have. It addresses points such as the basic security considerations and the main frauds that must be faced.

**Link:** https://www.incibe.es/protege-tu-empresa/

## LISA Institute Weekly Newsletter

The LISA Institute publishes the Weekly Newsletter, a brief summary of the news that have marked the agenda during the last seven days and with which you can be informed of different security, intelligence, cybersecurity, and geopolitical issues.

**Link:** https://www.lisainstitute.com/blogs/




NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com