DIVD

Annual Report 2023

Date	**23 February 2024**
Author	Chris van 't Hof
Version	1.0

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Introduction

The mission of the DIVD is to enhance digital safety by investigating vulnerabilities in information systems, reporting discovered issues to relevant parties, and offering help in resolving them. In our vision, we provide a supportive environment for volunteers who wish to contribute to this mission. They can work together, learn from one another, and receive assistance from other volunteers, paid staff members, and advanced technology. As an independent institute with its own Code of Conduct, DIVD does not act on behalf of others. We offer unsolicited help to anyone without exception and collaborate with a variety of partners to achieve our objectives. We consider DIVD as the volunteer fire brigade of the internet.

Scanning and notifying vulnerabilities

In 2023, DIVD CSIRT handled 37 cases and alerted the owners of 337,027 vulnerable IP-addresses of a Common Vulnerability and Exposure (CVE) along with guidance on how to address the issue. A comprehensive list of these incidents can be found in the appendix. Some notable cases are:

- DIVD-2023-00001-CITRIX SYSTEMS VULNERABLE FOR CVE-2022-27510. Thanks to Fox-IT's scans, we had historical data for the first time and could really see the impact of our reports. Impressive to see how the number of vulnerable instances decreased after an email round from us.
- 2023-00033-CITRIX SYSTEMS EXPLOITED WITH CVE-2023-3519. We scanned together with Fox-IT for Citrix devices that were already actually compromised, not just vulnerable.
- OS-Nexus Quantastor product warning, for the first time, after a year and a half of trying to collaborate with a vendor, we have really not succeeded and issued a product warning.

Collaboration and partnerships in this process have significantly improved. We collaborate more with cyber security businesses on fingerprinting vulnerabilities. Our notifications are currently forwarded by 20 GovCERT around the world, such as NCSC-UK, CISA in the USA, CBB in Belgium. First contacts were also made with the German GovCERT at the Bundesministerium.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Our researchers also found new vulnerabilities. This is our second line of research. DIVD has the status of CNA: a CVE Numbering Authority. This team has published 14 CVEs 2023. The final number will actually be higher, as CVEs are only published after the entire disclosure process with the vendor has been completed, so there may be even more CVEs reserved and awarded, but we are not yet publishing about this because the disclosure and fix have not yet been completed.

Our third line of research involves individual notification of open databases and leaked credentials. For example, we found many open Github repositories and Amazon S3 buckets, containing sensitive personal data and also username password combinations. Although the number of persons to be found in these sources runs in the thousands, we count these notifications as just one. Following our Code of Conduct, we only notify the owner of the systems and do not publish these findings.

The CSIRT has grown considerably over the past year, mainly due to several DIVD employees who have switched from the Research & Development department to the CSIRT. These people have helped enormously by immediately jumping into the deep end and taking a large number of fingerprints. developing and running cases.

Maintaining an environment where helpful hackers can do their thing

During 2023 DIVD grew from: 96 to 133 volunteers. We also improved the onboarding process of new volunteers with a registration system, containing many tick boxes of tasks, among which also a screening procedure and a legally binding statement of conduct (“VOG, or Verklaring Omtrent Gedrag” in Dutch). New recruits also can only start after signing a volunteer agreement, stating they will commit to the DIVD Code of Conduct. We deliberately put in more thresholds to keep hackers with bad intentions or people who only join because it may look good on their CV to enter the organization. With our growing reputation, DIVD can afford to only select the highly motivated helpful hackers.

Once on board, new volunteers join a team within one of the departments, receive an introduction training and handbook, are introduced to the rest of the organization at the General Meetings, in Team meetings and on Slack. Most of them land at the Research & Development department, our biggest department, but are free to move on to other departments as many of them did to IT and CSIRT. Meanwhile, they are offered an increasing number of opportunities to receive training in many areas..

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Due to our financial setbacks, we had to limit the hired staff to the bare minimum: just a bookkeeper and accountant. While part of our management team was partly paid in 2022, we decided at the start of 2023 we all needed to go back to being volunteers to save some budget for volunteer allowances, insurances, training, merchandise, events and above all: technology.

IT is perhaps the most important aspect for hackers to feel at home in our DIVD environment. Our scanning infrastructure has been functioning the whole 2023 without any unplanned outages. Moving our scan servers from one data center to another and implementing new hardware proceed without interrupting the core process of scanning the internet. Around this stable core process, we have been experimenting with quite some office applications with varying results, but never running the organization into any unnecessary risk.

Finally, a good environment also means a safe environment. The Security Office, consisting of a CISO and two ISOs, has been active during 2023 streamlining our IT environment and procedures based on the ISO27001 standard. Together with our Privacy Office, Data Protection Officer, Crisis Manager and Managing Director they form the department Governance, Risk and Compliance and cyclically maintained an Information Security Management System, Risk Matrix and Business Continuity Plan. The department People & Culture extended the number of Confidentiality Counselors from 2 to 4. Still, they have had no cases of jet.

In January 2024, we held our annual Volunteer Satisfaction Questionnaire (n=34). Despite our efforts to improve onboarding and collaboration after the results of last year, this year's results show a similar image. The following points stood out:

- It is clear what the DIVD stands for and the respondents have also joined the DIVD to shape that part of safer internet and giving back to society.
- Onboarding in 2023 was often experienced as messy and/or unclear.
- The average respondent spends 4 to 8 hours per week on the DIVD and this also corresponds to what they would like/be able to do.
- In general, they are satisfied with the team they are in and the team meetings are well appreciated.
- There could be more cooperation between teams, but at the moment they are often islands.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

- Communication with each other works well via Slack, but this is not collaborative. This is an area for improvement for 2024 that projects may help with.
- The MT is well known and can be found.
- People are most proud of the way in which DIVD has bounced back from the crisis situation at the beginning of 2023
- People feel the support in both carrying out the tasks and in being themselves and feel free to ask for help. There is a need for coaches and buddies and also some appreciation.

Transition from DIVD 2.0 to 3.0

Each year, in May, the Management Team retreats for a reflective session to review our organization's past and future. This year, we faced several challenges. Firstly we experienced a significant drop in income, due to a partner withdrawing their sponsorship out and an unexpected tax bill over 2022. Secondly, the two-tier structure with a supervisory board above the regular board, did not perform as anticipated . Third, even though the volunteer satisfaction survey showed people felt very much at home at DIVD, some stated they had trouble finding the right jobs and saw room for improvement in the collaboration among departments.

Therefore the Management Team went back to the drawing board to redesign our way of working to make DIVD more future proof and increase satisfaction and productivity of our volunteers. The input was provided by a working group with a representation of our volunteers who compared DIVDs organizational structure to that of other voluntary organizations. Because the organizational structure of DIVD in 2022, a line organization with departments and managers, was called DIVD 2.0, we called this redesign DIVD 3.0A transition manager was appointed who kept track of progress in tasks in weekly sprints and reported on the results to all the stakeholders. Some significant changes we achieved include:

DIVD 2.0	DIVD 3.0
Line organization: MT, departments and fixed positions.	Matrix organization with a Project Office running projects and members across departments
Researchers start cases, CSIRT follows up with notifications.	CSIRT is our core process, being supported by other departments.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Single sign on to DIVD environment	Identity & Access Management policy based on attributes
Heads of departments are also coaching their volunteers	A group of coaches will coach volunteers across departments
Financial dependency and fluctuation due to a small group of funders	A healthy mix of a larger group of funders to spread risk and build stability
Detailed and negotiated annual plans	Long term vision, more general annual plan and agile projects
one on one relationship management partners by director	Team Public Relations consisting of director, communications and content specialist.
Two-tier governance model: Supervisory Board, board and director	One-tier model with a larger board, director and Advisory Board.

Collaborations and partnerships

Our solid partnerships with IT security companies

Let's first mention the IT partners that have been with us for a long time. IT services company Schuberg Phillis has been supportive to DIVD from the start on, hosting our scan servers and providing personnel. Due to their shift in strategy to the cloud, Schuberg Philis moved away from its data centers and our servers needed to move. We found A2B Internet willing to provide us with a sponsored server rack, while Schuberg Phillis helped out during the transition that went quite smoothly thanks to our other partner LinProfs that provides valuable support in systems engineering. VMware helped DIVD out by funding new servers and support on acquiring and installing them. ESET, which also helped us acquire our own Autonomous System for our own IP addresses, kept supporting DIVD during 2023 with funding, services and their office for our annual partnerday. Also, BIT, supported DIVD with sponsored mailing services, as in previous years. Protect4Us joined as an IT partner in 2023, providing funding and expert knowledge on SAP systems.

For Addessium, 2023 was their second year of support to DIVD. This philanthropic fund not only provides funding, but also (re-)organizational advice on governance and

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

finance. As did the Limelight Foundation for 2022, but unfortunately they decided to stop funding DIVD in 2023.

Improved cooperation with governments

As mentioned in the CSIRT section, our relationship with governments significantly improved during 2023. A growing number of Governmental CERTs around the world is forwarding our notifications to their constituencies and sharing threat intelligence with us so we can prioritize the vulnerabilities we scan for.

A special mention here of the Dutch government. From our start on, several ministries and institutions such as National Cyber Security Center (NCSC), Digital Trust Center (DTC), police and the Public Prosecution Office, have been supportive of our work. Still, they showed little cooperation in the most important part of our work: forwarding notifications. This was hampered by legal boundaries of the NCSC. In a nutshell: the mandate of the National Cyber Security Center only covered organizations that were labeled 'national government' or 'critical infrastructure', but the CERT was not allowed to share which IP addresses they have, as this is marked as classified information. The NCSC has a legal basis to inform critical providers, government organizations and other chain organizations within the Nationwide Network of Cybersecurity Partnerships (LDS). NCSC could not always provide threat and incident information to the other chain organizations, due to boundaries within the law.

The boundaries were almost completely undone in December 2022 by an amendment to the law. This allows the NCSC to share threat and incident information in a broader sense with so-called chain organizations and in special cases with other providers. A special case exists if there is no chain organization and the information is about a threat or incident with significant consequences for the continuity of service of the provider.

After the merger between NCSC, Digital Trust Center and CSIRT-DSP was announced, it was concluded that their combined mandate includes all Dutch IP addresses. These parties already are working more closely together. This collaboration allows more organizations to be reached, including the non-vital business community - the DTC's target sector. During the summer, two large cases, Fortinet and Citrix, were the proof of that. DTC contacted all Dutch victims on our notifications.

With the start of the first minimal viable product for Victim and Target Notification, The Dutch Security Hotline (securitymeldpunt.nl) which served as an alternative route to notify the Netherlands therefore lost its operational urgency. DIVD has been setting up this

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

clearinghouse together with NBIP, Connect2Trust, Surf and AMS-IX, with funding by SIDN Fonds. Still, this work was not for nothing, it rather served as a strong signal on the urgency of organizing notifications. But now the NCSC and DTC follow the notifications, DIVD can focus its energy on the rest of the CERTs in the world.

Parallel to these cooperation developments, a parliamentary debate on the relation between DIVD and the Dutch government came to a closure. During a debate in 2022, the Dutch Minister of Justice & Security stated DIVD fulfills an important function in cybersecurity by scanning and notifying – in a way the government is not allowed to do. Members of Parliament then argued DIVD should be helped to receive funding for the work we do.

The minister assigned the NCTV, National Coordinator for Safety and Counter Terrorism, to follow up on the parliamentary request. During our first meetings, their legal advisors took the position that a government may not be allowed to fund an organization that does something the government itself is not allowed to do, calling it a possible 'U-turn construction'. The NCTV presented the issue to the Public Prosecution Office. They concluded: if we look at DIVDs Code of Conduct, their work is perfectly in line with the guidelines we set on Coordinated Vulnerability Disclosure, so there are no legal impediments to fund DIVD. We filed a budget plan for 2023-2025, which was approved and awarded in December 2023.

Sharing our knowledge and mission at events

Most of the work of DIVD is online, but now and then our members participate in cyber security conferences, hacker events and guest lectures, such as:

- 10 -12 february Hacker Hotel: several presentations and hacker activities delivered by DIVD
- 17 March Security Academy Unlocked: co hosted by Schuberg Phillis at their facility, DIVD provided a program together with the Security Academy for their alumni.
- 31 March NCSC/DIVD meet-up: operational experts from both organizations meeting and doing a pub quiz.
- 11 May Hack010: 9 hackers from DIVD joined in a bugbounty challenge organized by the municipality of Rotterdam and won prizes.
- 10 August ODNI Group, presentation DIVD scanning and notifying.
- 7 September Anti Abuse Network AAN: presentation on DIVD3.0.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

- 1 October Hack The Hague: 11 hackers from DIVD joined in a bug bounty challenge organized by the municipality of The Hague and won prizes.
- 2-4 October ONE expo stand. Many volunteers from DIVD were present at the conference each day at a stand to talk about our work and meet current and new partners.
- 13-15 November ISIDOOR: DIVD joined the national cyber security crisis event with response cells, scenario building and evaluation.
- 4 december was HCC-Noord: presentation on phishing and steganography
- 27-30 December Chaos Computer Congress: a series of four workshops on how we scan and notify.
- Several guest lectures at schools and universities: IT-vitae 23 March, Faculty of Criminology at Leiden University 5 December.

DIVD events:

- 19 May, Management Day: strategic management retreat.
- 26 September DIVD Partner Event: bbq, meet-up and speeches by DIVD for all DIVD partners, at ESET HQ Sliedrecht.
- 1 December End of the Year Event: 50 DIVD volunteers present with pizza, pub quiz, fire breathing and disco at Hack42 Arnhem.

The DIVD Board

In the past year (2023), DIVD underwent significant changes in the areas of governance and supervision. Under the supervision of the board, the following transitions were coordinated and implemented:

- **Transition to DIVD 3.0:** The transition plan DIVD 3.0 was designed and implemented. In this transition plan, DIVD opted for a one-tier governance model and dissolved the Supervisory Board (RvT) by mutual agreement.
- **Vision 2023-2026:** DIVD offers volunteers who want to contribute to our mission an environment where they can work and learn from each other. The DIVD board created a vision document for 2023-2026 based on nine pillars that guide the practice of our Management Team and volunteers. This board will review this vision yearly to accommodate changes because of the fast-changing nature of our profession. A summary of the changes per pillar:

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

- *Safe and trusted environment*: DIVD is a safe environment and recognized as such, made possible by the Code of Conduct we have agreed and signed with each other and by the presence of confidential counselors and complaints procedures.
- *Ethical values and new initiatives*: DIVD acts as the mothership from which various new initiatives emerge based on our strong ethical values.
- *Robust organizational structure*: In 2026, a solid organizational structure will be in place that ensures that DIVD continues to function, even when there is a high turnover of volunteers.
- *Automated and documented processes*: DIVD strives for automated, documented, and clear processes for everyone within the organization. This allows us to work efficiently, be adaptive to new developments, and continuously improve for the benefit of quality and our stakeholders.
- *Strategic planning and implementation*: DIVD has developed robust processes to strategically plan and implement its strategy on time and within budget.
- *Transparency, innovation and collaboration:* DIVD strives for a transparent, innovative and agile organizational culture involving all volunteers.
- *Personal development and appreciation:* DIVD is where volunteers want to be and stay, because they can learn from and teach others here.
- *Financial independence and stability:* DIVD strives for a fixed income stream that is not dependent on one specific source, such as subsidies, donations, or project funds, but a healthy mix.
- *Robust risk management:* DIVD has a robust risk management policy to identify, analyze, and manage potential threats. We strive for a culture in which risk awareness is central and in which we proactively take measures to minimize risks and keep them manageable.

- **New chair and a renewed Board:** At the end of 2023 the DIVD Board has six members consisting of a chair, a secretary, a treasurer, and three general board members. In Q4 2023, Inge Bryan took over the chairmanship from Astrid Oosenbrug, and Tom van Dael joined DIVD as a general board member with a strategic commercial and finance portfolio. A complete list of the board members, including their roles, can be seen below.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Board Member	Role
Inge Bryan	Chair
Shairesh Algoe	Treasurer and acting chair replacement
Eleonora Petridou	Secretary
Joost Hendricksen	General Board Member & IT Portfolio
Marinus Kuivenhoven	General Board Member
Tom van Dael	Strategic Commercial and Finance Portfolio

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Appendix 1: Cases in 2023

Cases still open at 31 December 2023

DIVD-2023-00045 - CONFLUENCE RCE VULNERABILITY IN CONFLUENCE DATA CENTER AND CONFLUENCE SERVER

Wessel Baltus

Confluence Data Center and Server RCE vulnerability allow an authorized user, including one with anonymous access, to inject unsafe user input into a Confluence page
More

DIVD-2023-00042 - CONFLUENCE IMPROPER AUTHORIZATION VULNERABILITY

Wessel Baltus

Confluence Data Center and Server allow unauthorized users to set Confluence in setup mode leading to the possibility to create administrator accounts that have the capabilities for RCE
More

DIVD-2023-00040 - CRITICAL F5 BIG-IP UNAUTHENTICATED RCE VULNERABILITY

Boaz Braaksma

This vulnerability (CVE-2023-46747) may allow an unauthenticated adversary with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands."
More

DIVD-2023-00039 - VMWARE VCENTER SERVER RCE

Max van der Horst

VMware has released security updates for vCenter Server that could result in Remote Command Execution.
More

DIVD-2023-00038 - GLOBAL CISCO IOS-XE (CVE-2023-20198) IMPLANTS

Max van der Horst

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

An unknown threat actor is using a recent authentication bypass vulnerability (CVE-2023-20198) on Cisco IOS-XE to backdoor Cisco appliances worldwide.
More

DIVD-2023-00035 - REMOTE CODE EXECUTION IN JUNIPER NETWORKS SRX- AND EX-SERIES

Max van der Horst

By chaining multiple vulnerabilities an attacker is able to execute arbitrary code or commands via specifically crafted requests.
More

DIVD-2023-00032 - ACCESS CONTROL BYPASS - CVE-2023-29298 & CVE-2023-38205

Finn van der Knaap

Both vulnerabilities allow an attacker to bypass the product feature that restricts external access to the ColdFusion Administrator.
More

DIVD-2023-00030 - CITRIX SYSTEMS VULNERABLE FOR CVE-2023-3519

Lennaert Oudshoorn

DIVD is notifying owners of vulnerable Citrix ADC and Gateway systems, based on scanning data obtained from Fox-IT.
More

DIVD-2023-00028 - SQL INJECTION IN MOVEIT TRANSFER - CVE-2023-36934

Célistine Oosting

A new SQL Injection vulnerability has been found in MOVEit Transfer.
More

DIVD-2023-00027 - IGNITE REALTIME OPENFIRE AUTH BYPASS - CVE-2023-32315

Hans Meuris

Ignite Realtime Openfire version 3.10.0 through 4.6.8 (excluded) and 4.7.0 to 4.7.5 (excluded) are vulnerable to a Path traversal vulnerability
More

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

DIVD-2023-00026 - APACHE SUPERSET AUTHENTICATION BYPASS LEADS TO RCE - CVE-2023-27524

Finn van der Knaap

Apache Superset, up to and including 2.0.1 vulnerable to bypass that can lead to an RCE.
More

DIVD-2023-00010 - REMOTE CODE EXECUTION IN MICROSOFT EXCHANGE SERVER

Célistine Oosting

Remote Code Execution vulnerability was found and fixed in Microsoft Exchange Server, the DIVD is scanning for vulnerable systems and notifying owners of vulnerable systems
More

DIVD-2023-00002 - PUBLICLY REACHABLE MALICIOUS WEBSHELLS

Max van der Horst

DIVD is searching the Internet for publicly reachable malicious webshells.
More

Closed cases

DIVD-2023-00036 - AUTHENTICATION BYPASS IN JETBRAINS TEAMCITY

Max van der Horst

Successful exploitation of CVE-2023-42793 allows an unauthenticated attacker with HTTP(S) access to a TeamCity server to perform a remote code execution attack and gain administrative control of the server.
More

DIVD-2023-00034 - API AUTHENTICATION BYPASS VULNERABILITY IN IVANTI SENTRY

Max van der Horst

Ivanti Sentry has an API authentication bypass vulnerability with CVSS 9.8. System owners are advised to limit access to port 8443.
More

DIVD-2023-00033 - CITRIX SYSTEMS EXPLOITED WITH CVE-2023-3519

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Max van der Horst

DIVD is notifying owners of exploited Citrix ADC and Gateway systems, based on scanning data obtained from Fox-IT.
More

DIVD-2023-00031 - IVANTI MOBILEIRON VULNERABLE FOR CVE-2023-35078

Lennaert Oudshoorn

DIVD is notifying owners of vulnerable Ivanti MobileIron
More

DIVD-2023-00029 - CRITICAL FORTINET SSL-VPN RCE VULNERABILITY

Boaz Braaksma

A heap-based buffer overflow vulnerability [CWE-122] in FortiOS and FortiProxy SSL-VPN may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests.
More

DIVD-2023-00025 - MULTIPLE VULNERABILITIES IN DANFOSS AK-SM800A

Max van der Horst

Danfoss AK-SM800A has multiple web-related vulnerabilities. It is advised to install the provided patch.
More

DIVD-2023-00024 - SQL INJECTION IN GEOSERVER - CVE-2023-25157

Jeroen van de Weerd

GeoServer has a critical SQL injection vulnerability.
More

DIVD-2023-00023 - SQL INJECTION IN MOVEIT TRANSFER - CVE-2023-34362

Max van der Horst

MOVEit Transfer has a critical SQL injection vulnerability that is actively exploited for data theft.
More

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

DIVD-2023-00022 - OS COMMAND INJECTION VULNERABILITY OF ZYXEL FIREWALLS

Stan Plasmeijer

Zyxel has released patches for an OS command injection vulnerability found by TRAPA Security and urges uses to install them for optimal protection.
More

DIVD-2023-00021 - MULTIPLE VULNERABILITIES IN DANFOSS AK-EM 100

Max van der Horst

Danfoss AK-EM 100 has multiple web-related vulnerabilities. It is advised to phase out this product, as this product is End of Life.
More

DIVD-2023-00020 - PAPERCUT MF/NG AUTHENTICATION BYPASS

Max van der Horst

This vulnerability allows remote attackers to bypass authentication on affected installations of PaperCut MF/NG 22.0.5 (Build 63914).
More

DIVD-2023-00017 - CISCO SMALL BUSINESS ROUTER AUTHENTICATION BYPASS

Max van der Horst

Cisco RV016, RV042, RV042G and RV082 contain an authentication bypass vulnerability.
More

DIVD-2023-00016 - GLPI REMOTE CODE EXECUTION

Finn van der Knaap en Josha Beekman

GLPI version below 9.5.9 & 10.0.3 are vulnerable to Remote Code Execution
More

DIVD-2023-00015 - YEASTAR CONFIGURATION PANEL TAKEOVER

Rutger Hermens

Yeastar N412 and N824 Configuration Panels are vulnerable to unauthenticated account takeover.
More

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

DIVD-2023-00014 - CRITICAL BROKEN AUTHENTICATION FLAW IN JIRA SERVICE MANAGEMENT PRODUCTS

Rutger Hermens

Vulnerable Jira Service Management Server and Data Center versions allow an attacker to impersonate another user and gain access under certain circumstances.
More

DIVD-2023-00012 - UNAUTHENTICATED REMOTE COMMAND EXECUTION IN IBM ASPERA FASPEX

Axel Boesenach

IBM Aspera Faspex 4.4.1 could allow a remote attacker to execute arbitrary code on the system, caused by a YAML deserialization flaw. By sending a specially crafted obsolete API call, an attacker could exploit this vulnerability to execute arbitrary code on the system.
More

DIVD-2023-00011 - FORTINAC AND FORTIWEB RCE VULNERABILITY

Max van der Horst

Fortinet has released security updates for its FortiNAC and FortiWeb products to fix two critical vulnerabilities.
More

DIVD-2023-00009 - CISCO RV SERIES REMOTE COMMAND EXECUTION

Max van der Horst

Cisco RV340, RV340W, RV345 and RV345P contain a Remote Command Execution vulnerability.
More

DIVD-2023-00007 - GLOBAL VMWARE ESXI RANSOMWARE ATTACK

Max van der Horst

Criminals are attacking VMware ESXi servers vulnerable to CVE-2021-21974 worldwide to deploy ransomware.
More

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

DIVD-2023-00006 - UNAUTHENTICATED CODE INJECTION IN QNAP QTS AND QUTS HERO

Stan Plasmeijer

QNAP has released an advisory for devices running QTS 5.0.1 and QuTS hero h5.0.1. Those devices might be vulnerable for code injection.
More

DIVD-2023-00004 - UNAUTHENTICATED REMOTE COMMAND EXECUTION USING SAML IN ZOHO MANAGEENGINE

Max van der Horst

Use of outdated Apache Santuario library in Zoho ManageEngine causes an unauthenticated RCE vulnerability by sending a malicious SAML response.
More

DIVD-2023-00003 - OS COMMAND INJECTION IN CENTOS CWP

Max van der Horst

The login/index.php endpoint in CentOS Control Web Panel 7 before 0.9.8.1147 allows unauthenticated attackers to execute OS commands.
More

DIVD-2023-00001 - CITRIX SYSTEMS VULNERABLE FOR CVE-2022-27510 AND/OR CVE-2022-27518

Frank Breedijk

Based on scanning data obtained from Fox-IT, DIVD is notifying owners of vulnerable Citrix ADC and Gateway systems
More

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl