2017 News — Archive

Minutes from CVE Board Teleconference Meeting on December 13 Now Available
December 26, 2017

The CVE Board held a teleconference meeting on December 13, 2017. Read the meeting minutes.

Important Message About Our @CVEnew Twitter Account
December 20, 2017

We recently identified a Twitter handle impersonating our @CVEnew handle. Twitter was notified and suspended the impersonating handle. Follow https://twitter.com/CVEnew for regular CVE Entry updates.

Minutes from CVE Board Teleconference Meeting on November 29 Now Available
December 12, 2017

The CVE Board held a teleconference meeting on November 29, 2017. Read the meeting minutes.

New CVE Board Member from IBM
December 4, 2017

Scott Moore of IBM has joined the CVE Board.

Read the full announcement and welcome message in the CVE Board email discussion list archive.

Minutes from CVE Board Teleconference Meeting on November 15 Now Available
November 28, 2017

The CVE Board held a teleconference meeting on November 15, 2017. Read the meeting minutes.

Minutes from CVE Board Teleconference Meeting on November 1 Now Available
November 13, 2017

The CVE Board held a teleconference meeting on November 1, 2017. Read the meeting minutes.

SAP Added as CVE Numbering Authority (CNA)
November 9, 2017

SAP SE is now a CVE Numbering Authority (CNA) for all SAP products.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 81 organizations currently participate as CNAs: Adobe; Airbus; Alibaba; Apache; Apple; ASUSTOR; Atlassian; Autodesk; BlackBerry; Booz Allen Hamilton; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Forcepoint; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; Kaspersky; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; NetApp; Netflix; Netgear; Node.js; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; QNAP; Qualcomm; Rapid 7; Red Hat; Riverbed; SAP; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; Tenable; TIBCO; Trend Micro; VMware; Yandex; Zephyr Project; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Booz Allen Hamilton Added as CVE Numbering Authority (CNA)
November 7, 2017

Booz Allen Hamilton, Inc. is now a CVE Numbering Authority (CNA) for all Booz Allen Hamilton products as well as vulnerabilities in third-party software discovered by Booz Allen Hamilton that are not covered by another CNA.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 80 organizations currently participate as CNAs: Adobe; Airbus; Alibaba; Apache; Apple; ASUSTOR; Atlassian; Autodesk; BlackBerry; Booz Allen Hamilton; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Forcepoint; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; Kaspersky; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; NetApp; Netflix; Netgear; Node.js; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; QNAP; Qualcomm; Rapid 7; Red Hat; Riverbed; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; Tenable; TIBCO; Trend Micro; VMware; Yandex; Zephyr Project; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Minutes from CVE Board Teleconference Meeting on October 18 Now Available
October 26, 2017

The CVE Board held a teleconference meeting on October 18, 2017. Read the meeting minutes.

Node.js Added as CVE Numbering Authority (CNA)
October 25, 2017

Node.js is now a CVE Numbering Authority (CNA) for all actively developed versions of software developed under the Node.js project on https://github.com/nodejs.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 79 organizations currently participate as CNAs: Adobe; Airbus; Alibaba; Apache; Apple; ASUSTOR; Atlassian; Autodesk; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Forcepoint; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; Kaspersky; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; NetApp; Netflix; Netgear; Node.js; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; QNAP; Qualcomm; Rapid 7; Red Hat; Riverbed; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; Tenable; TIBCO; Trend Micro; VMware; Yandex; Zephyr Project; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

CVE Overview for Prospective CNAs Document Now Available
October 17, 2017

The CVE Overview for Prospective CNAs document is now available on the CVE website. The purpose of this document is to describe the roles and responsibilities of a CVE Numbering Authority (CNA) such that a decision can be made whether to pursue becoming a CNA.

Specifically, this document includes detailed information about the following:

- Conceptual Basis of CVE
- Design and Operational Choices for CVE – CVE Entries Purposely Provide Minimal Information About a Vulnerability, The CVE List is a Simple List, CVE Only Publishes Already-Disclosed Vulnerabilities, and The Anatomy of a CVE Entry - Example
- CVE and the National Vulnerability Database (NVD)
- CVE and CNAs – Sources of Vulnerability Information, Benefits of Early CVE ID Assignment, Roles and Responsibilities of a CVE CNA - High Level View, and Benefits of Operating as a CNA
- Special Considerations for Prospective CNAs – Requirements for Assigning a CVE ID and Challenges When Assigning CVE IDs
- Acronyms
- References

Visit the Documentation for CNAs section for additional information for CNAs. You may also contact us with any comments or questions.

NetApp Added as CVE Numbering Authority (CNA)
October 13, 2017

NetApp, Inc. is now a CVE Numbering Authority (CNA) for all NetApp products, as well as projects hosted on https://github.com/netapp. CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 78 organizations currently participate as CNAs: Adobe; Airbus; Alibaba; Apache; Apple; ASUSTOR; Atlassian; Autodesk; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Forcepoint; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; Kaspersky; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; NetApp; Netflix; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; QNAP; Qualcomm; Rapid 7; Red Hat; Riverbed; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; Tenable; TIBCO; Trend Micro; VMware; Yandex; Zephyr Project; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Minutes from CVE Board Teleconference Meeting on October 4 Now Available
October 13, 2017

The CVE Board held a teleconference meeting on October 4, 2017. Read the meeting minutes.

ASUSTOR Added as CVE Numbering Authority (CNA)
October 5, 2017

ASUSTOR Inc. is now a CVE Numbering Authority (CNA) for its ASUSTOR network attached storage (NAS) products, as well as its ADM systems, NAS apps, mobile apps, and utilities.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 77 organizations currently participate as CNAs: Adobe; Airbus; Alibaba; Apache; Apple; ASUSTOR; Atlassian; Autodesk; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell

EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Forcepoint; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; Kaspersky; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netflix; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; QNAP; Qualcomm; Rapid 7; Red Hat; Riverbed; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; Tenable; TIBCO; Trend Micro; VMware; Yandex; Zephyr Project; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

CVE Replaces "CVE Compatibility Program" with CVE Compatibility Guidance Document
September 29, 2017

The previous formal CVE Compatibility Program of declarations and questionnaires has been discontinued, and all product listings from the program have been moved to "archive" status. The CVE Team will no longer accept declarations or questionnaires.

Instead, a *CVE Compatibility Guidelines* document is now available to assist you in making your product or service "CVE Compatible." This new guidance includes detailed information on the following topics: definitions, high-level guidelines, accuracy, documentation, CVE date usage, CVE syntax support, type-specific guidelines, and media guidelines.

If you have any comments or concerns about the discontinued program or the new guidance document, please use our CVE Request web form and select the Other request type to contact us.

Minutes from CVE Board Teleconference Meeting on September 20 Now Available
September 29, 2017

The CVE Board held a teleconference meeting on September 20, 2017. Read the meeting minutes.

Forcepoint Added as CVE Numbering Authority (CNA)
September 21, 2017

Forcepoint is now a CVE Numbering Authority (CNA) for Forcepoint products only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 76 organizations currently participate as CNAs: Adobe; Airbus; Alibaba; Apache; Apple; Atlassian; Autodesk; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Forcepoint; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; Kaspersky; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netflix; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; QNAP; Qualcomm; Rapid 7; Red Hat; Riverbed; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; Tenable; TIBCO; Trend Micro; VMware; Yandex; Zephyr Project; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Minutes from CVE Board Teleconference Meeting on September 6 Now Available
September 14, 2017

The CVE Board held a teleconference meeting on September 6, 2017. Read the meeting minutes.

1 Product from Bluedon Information Security Technologies Now Registered as Officially "CVE-Compatible"
September 14, 2017

One additional cyber security product has achieved the final stage of the CVE compatibility process and is now officially "CVE-Compatible." A total of 153 products to-date have been recognized as officially compatible.

The following product is now registered as officially "CVE-Compatible":

Bluedon Information Security Technologies Co., Ltd.	-	Bluedon Vulnerability Scanning System

To review all products and services listed, visit CVE-Compatible Products and Services.

Riverbed and Zephyr Added as CVE Numbering Authorities (CNAs)
September 8, 2017

Two additional organizations are now CVE Numbering Authorities (CNAs): Riverbed Technology, Inc. for Riverbed products only, and Zephyr Project for Zephyr project components and vulnerabilities that are not already covered by another CNA.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 75 organizations currently participate as CNAs: Adobe; Airbus; Alibaba; Apache; Apple; Atlassian; Autodesk; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; Kaspersky; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netflix; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; QNAP; Qualcomm; Rapid 7; Red Hat; Riverbed; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; Tenable; TIBCO; Trend Micro; VMware; Yandex; Zephyr Project; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Minutes from CVE Board Teleconference Meeting on August 23 Now Available
September 5, 2017

The CVE Board held a teleconference meeting on August 23, 2017. Read the meeting minutes.

QNAP Added as CVE Numbering Authority (CNA)
August 22, 2017

QNAP is now a CVE Numbering Authority (CNA) for its QTS, QES, and QVR products as well as its mobile apps and utilities.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 73 organizations currently participate as CNAs: Adobe; Airbus; Alibaba; Apache; Apple; Atlassian; Autodesk; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; Kaspersky; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netflix; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; QNAP; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; Tenable; TIBCO; Trend Micro; VMware; Yandex; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Minutes from CVE Board Teleconference Meeting on August 9 Now Available
August 16, 2017

The CVE Board held a teleconference meeting on August 9, 2017. Read the meeting minutes.

Airbus and Kaspersky Labs Added as CVE Numbering Authorities (CNAs)
August 10, 2017

Airbus and Kaspersky Labs are now CVE Numbering Authorities (CNAs). The scope for Airbus is all Airbus products as well as vulnerabilities in third-party software discovered by Airbus that are not covered by another CNA, and for Kaspersky Labs it is its B2C products (Kaspersky Free, Kaspersky Privacy Cleaner, Kaspersky Secure Connection, Kaspersky Password Manager, Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security, Kaspersky Password Manager, Kaspersky Safe Kids, Kaspersky Virus Scanner, Kaspersky Virus Scanner Pro, Kaspersky Security Scan, Kaspersky Software Updater, Kaspersky System Checker, Kaspersky AdCleaner, Kaspersky QR Scanner, Kaspersky Safe Browser, Kaspersky Threat Scan, Kaspersky Virus Removal Tool, and Kaspersky Rescue Disk) and B2B products (Kaspersky Small Office Security, Kaspersky Endpoint Security Cloud, Kaspersky Endpoint Security for Business Select, Kaspersky Endpoint Security for Business Advanced, Kaspersky Endpoint Security for Business Total, Kaspersky Security for Mail Server, Kaspersky Security for File Server, Kaspersky Security for Mobile, Kaspersky Security for Internet Gateway, Kaspersky Security for Virtualization, Kaspersky Security for Collaboration, Kaspersky Systems Management, Kaspersky Security for Storage, Kaspersky DDoS Protection, Kaspersky Embedded Systems Security, Kaspersky Anti-Targeted Attack Platform, Kaspersky Security Intelligence Services, Kaspersky Fraud Prevention, and Kaspersky Industrial CyberSecurity), as well as vulnerabilities discovered in third-party software not covered by another CNA.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 72 organizations currently participate as CNAs: Adobe; Airbus, Alibaba; Apache; Apple; Atlassian; Autodesk; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; Kaspersky; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netflix; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; Tenable; TIBCO; Trend Micro; VMware; Yandex; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Autodesk Added as CVE Numbering Authority (CNA)
August 9, 2017

Autodesk is now a CVE Numbering Authority (CNA) for all currently supported Autodesk applications and cloud services.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 70 organizations currently participate as CNAs: Adobe; Alibaba; Apache; Apple; Atlassian; Autodesk; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netflix; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; Tenable; TIBCO; Trend Micro; VMware; Yandex; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Alibaba Added as CVE Numbering Authority (CNA)
August 2, 2017

Alibaba, Inc. is now a CVE Numbering Authority (CNA) for projects listed on its Alibaba GitHub website only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 69 organizations currently participate as CNAs: Adobe; Alibaba; Apache; Apple; Atlassian; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netflix; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; Tenable; TIBCO; Trend Micro; VMware; Yandex; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Minutes from CVE Board Teleconference Meeting on July 26 Now Available
August 2, 2017

The CVE Board held a teleconference meeting on July 26, 2017. Read the meeting minutes.

Slides from "CVE IDs and How to Get Them" Talk at *DEF CON 25* Now Available
August 2, 2017

Briefing slides are now available from the CVE talk entitled "CVE IDs and How to Get Them" by CVE Numbering Authority Program Lead Dan Adinolfi and CVE Team Member Anthony Singleton on July 28, 2017 at the "Wall of Sheep" at *DEF CON 25* in Las Vegas, Nevada, USA.
Talk synopsis from the conference website: "The Common Vulnerabilities and Exposures (CVE) program uniquely identifies and names publicly-disclosed vulnerabilities in software and other codebases. Whether you are a vulnerability researcher, a vendor, or a project maintainer, it has never been easier to have CVE IDs assigned to vulnerabilities you are disclosing or coordinating around. This presentation will be an opportunity to find out how to participate as well as a chance to offer your thoughts, questions, or feedback about CVE. Attendees will learn what is considered a vulnerability for CVE, how to assign CVE IDs to vulnerabilities, how to describe those vulnerabilities within CVE ID entries, how to submit those assignments, and where to get more information about CVE assignment."

Visit the CVE Calendar for information on this and other events.

Minutes from CVE Board Teleconference Meeting on May 24 Now Available
August 2, 2017

The CVE Board held a teleconference meeting on May 24, 2017. Read the meeting minutes.

REMINDER: "REJECT" Is Not Always a Permanent State for a CVE ID Begins July 27, 2017
July 27, 2017

CVE IDs in the "REJECT" state can now be changed to another state at any time as appropriate.
Please see FOCUS ON: Marking a CVE ID "REJECT" Is Not Permanent; It Can Be Updated and Added to the CVE List for details.

Tenable Added as CVE Numbering Authority (CNA)
July 24, 2017

Tenable Network Security, Inc. is now a CVE Numbering Authority (CNA) for Tenable products and third-party products upon which they perform their vulnerability research that are not covered by another CNA.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 68 organizations currently participate as CNAs: Adobe; Apache; Apple; Atlassian; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netflix; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; Tenable; TIBCO; Trend Micro; VMware; Yandex; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Duo Added as CVE Numbering Authority (CNA)
July 18, 2017

Duo Security, Inc. is now a CVE Numbering Authority (CNA) for Duo products and any third-party research targets not covered by another CNA. CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 67 organizations currently participate as CNAs: Adobe; Apache; Apple; Atlassian; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Duo; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netflix; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; TIBCO; Trend Micro; VMware; Yandex; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Minutes from CVE Board Teleconference Meeting on July 12 Now Available
July 18, 2017

The CVE Board held a teleconference meeting on July 12, 2017. Read the meeting minutes.

Minutes from CVE Board Teleconference Meeting on June 28 Now Available
July 13, 2017

The CVE Board held a teleconference meeting on June 28, 2017. Read the meeting minutes.

ZTE Added as CVE Numbering Authority (CNA)
July 11, 2017

ZTE Corporation is now a CVE Numbering Authority (CNA) for ZTE products only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 66 organizations currently participate as CNAs: Adobe; Apache; Apple; Atlassian; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netflix; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; TIBCO; Trend Micro; VMware; Yandex; Zero Day Initiative; and ZTE.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

IMPORTANT: CVE Identifier (CVE ID) Reference Updates Begin on July 10, 2017
July 3, 2017

To help keep CVE ID References up-to-date within the CVE List, the CVE Team will be updating a large number of References where necessary in the coming months.

The CVE IDs affected include those from years 1999 through 2016. CVE List consumers will see up to 5,000 CVE IDs with updated references beginning on July 10, 2017. On 8-day intervals thereafter, additional batches of up to 5,000 CVE IDs with updated references will occur. These updates will occur indefinitely until further notice.

If you have any comments or concerns about this process, please send them to our CVE Request web form, and select the Other request type.

CVE Adds 3 New CVE Numbering Authorities (CNAs): Netflix, Trend Micro, and Zero Day Initiative
June 29, 2017

The following two software vendors and one third-party coordinator are now CVE Numbering Authorities (CNAs): Netflix, Inc. for Netflix Mobile Streaming Application and Netflix Open Source projects only; Trend Micro, Inc. for Trend Micro issues only; and Zero Day Initiative, as a third-party coordinator, for products and projects covered by its bug bounty programs not already covered by another CNA.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 65 organizations currently participate as CNAs: Adobe; Apache; Apple; Atlassian; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netflix; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; TIBCO; Trend Micro; VMware; Yandex; and Zero Day Initiative.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

FOCUS ON: Marking a CVE ID "REJECT" Is Not Permanent; It Can Be Updated and Added to the CVE List
June 27, 2017

The CVE Team and CVE Board have recently revisited the use of CVE Identifier (CVE ID) states — REJECT, RESERVED, DISPUTED — and are planning to make some necessary changes to them in the coming months.

One of the changes recently discussed was in how the "REJECT" state is applied, and specifically whether a REJECT CVE ID can change states again at a later date.

What REJECT Means for a CVE ID

As a recap, a CVE ID marked as REJECT is a CVE ID that is not accepted as a CVE ID. The reason a CVE ID is marked REJECT will most often be stated in the Description of the CVE ID. Possible examples include it being a duplicate CVE ID, it being withdrawn by the original requester, it being assigned incorrectly, or some other administrative reason.

As a rule, REJECT CVE IDs should be ignored. However, there may be cases where a CVE ID previously marked as REJECT might need to move back to RESERVED or a populated state (i.e., the details and References are published and included).

A REJECT State Is Not Permanent

The CVE Team and CVE Board agree that the REJECT state should NOT be considered permanent, and that changes to this CVE ID state should be allowed in the future.

An example case could include a simple accidental REJECT, where a CVE ID was marked as REJECT by a CVE Numbering Authority (CNA) but the CVE ID was used publicly. In this case, it would create more confusion and additional work to REJECT the already used CVE ID, assign a new CVE ID, and also make sure that all public references are updated. The change discussed here would be to simply change the REJECT CVE ID and populate it with the details that were intended.

Both the CVE Team and CVE Board agree that some downstream consumers of CVE may be currently interpreting the REJECT state as permanent and that the CVE ID will never change in the future. It was also agreed that we should provide proper notice to the community that this change in use of the REJECT state should be provided.

Moving Forward

This announcement serves as notice that beginning July 27, 2017, CVE IDs in the REJECT state can be changed to another state at any time as appropriate.
If you have any comments or concerns about this change, please send them to our CVE Request web form, and select the Other request type.

Atlassian Added as CVE Numbering Authority (CNA)
June 12, 2017

Atlassian is now a CVE Numbering Authority (CNA) for Atlassian issues only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 62 organizations currently participate as CNAs: Adobe; Apache; Apple; Atlassian; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

CA Technologies Added as CVE Numbering Authority (CNA)
June 5, 2017

CA Technologies is now a CVE Numbering Authority (CNA) for CA Technologies issues only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 61 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Dahua Added as CVE Numbering Authority (CNA)
June 5, 2017

Dahua Technologies is now a CVE Numbering Authority (CNA) for Dahua issues only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 61 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; CA; Canonical; CERT/CC; Check Point; Cisco; Dahua; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Synology Added as CVE Numbering Authority (CNA)
June 1, 2017

Synology Inc. is now a CVE Numbering Authority (CNA) for Synology issues including its network attached storage (NAS) products only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 59 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; Canonical; CERT/CC; Check Point; Cisco; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Synology; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Minutes from CVE Board Teleconference Meeting on May 3 Now Available
June 1, 2017

The CVE Board held a teleconference meeting on May 3, 2017. Read the meeting minutes.

Ambionics Security Makes Declaration of CVE Compatibility
May 22, 2017

Ambionics Security declared that its Ambionics Security Service is CVE-Compatible. For additional information about this and other CVE-Compatible products, visit the CVE-Compatible Products and Services section.

Bluedon Information Security Technologies Makes Declaration of CVE Compatibility
May 22, 2017

Bluedon Information Security Technologies Co., Ltd. declared that its Bluedon Vulnerability Scanning System is CVE-Compatible. For additional information about this and other CVE-Compatible products, visit the CVE-Compatible Products and Services section.

New CVE Board Member from Lenovo
May 11, 2017

Beverly Finch of Lenovo Group Ltd. has joined the CVE Board.

Read the full announcement and welcome message in the CVE Board email discussion list archive.

IMPORTANT: CVE Will Reject a Group of Unused CVE IDs on May 11
May 10, 2017

To help reduce the number of reserved but unused CVE IDs in the CVE List, the CVE Team will reject CVE IDs that CVE Numbering Authorities (CNAs) have indicated as being unused from their prior CVE ID allocations.

The CVE IDs affected include those from years 1999 through 2016. CVE List consumers will see 3,306 reserved CVE IDs become rejected in an update on May 11, 2017.

What to Expect

Once these CVE IDs are rejected, the Description portion of each CVE ID will be updated with the text below, with [Year] replacing the four-digit year:

** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during [Year]. Notes: none.

For additional information about CVE IDs marked as RESERVED and REJECT, please see Why is a CVE entry marked as "RESERVED" when a CVE ID is being publicly used? and What does it mean when a CVE Identifier is marked "REJECT"?.

Moving Forward

Each year, CNAs are given blocks of CVE IDs that are marked as "RESERVED" in the CVE List until they are assigned to a vulnerability and published. CNAs often do not use all the CVE IDs they are allocated, which means many reserved CVE IDs that will never be assigned to a vulnerability. As a result, the unused CVE IDs need to be moved from RESERVED to REJECT status to avoid confusion and make it clear to CVE List consumers that the unused CVE IDs do not represent unannounced vulnerabilities.

Moving forward, the CVE Team will now ask CNAs for their lists of unused CVE IDs from their allocations at the start of each new calendar year, and those unused CVE IDs will be updated to "REJECT" status at that time.

If you have any comments or concerns about this process, please contact us using the CVE Request web form.

Elastic Added as CVE Numbering Authority (CNA)
May 4, 2017

Elastic is now a CVE Numbering Authority (CNA) for Elasticsearch, Kibana, Beats, Logstash, X-Pack, and Elastic Cloud Enterprise products only. CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 58 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; Canonical; CERT/CC; Check Point; Cisco; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Eclipse Foundation; Elastic; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

"Expanding and Improving" CVE Talk at *European Government CERTs (EGC) Group Meeting* on May 18
May 4, 2017

CVE Numbering Authorities Program Lead Dan Adinolfi will give a talk entitled "Expanding and Improving CVE to Facilitate Vulnerability Disclosure and Management" on May 18, 2017 at the *European Government CERTs (EGC) Group Meeting* in The Hague, the Netherlands.
Talk synopsis: "The Common Vulnerabilities and Exposures (CVE) program uniquely identifies and names publicly-disclosed vulnerabilities in software and other codebases. CVE Numbering Authorities (CNAs) are an important part of the CVE program and are given the ability to identify and name CVE IDs in coordination with the MITRE CVE team. Participating as a CVE CNA allows organizations to have more control over their vulnerability management and disclosure processes while also ensuring a consistent level of service and a high quality of content within the CVE list. Becoming a CNA can be beneficial to vendors, coordination centers, and their customers, and it helps build a community of practice that continues to help improve the state of vulnerability management across many sectors."

Visit the CVE Calendar for information on this and other events.

"Expanding and Improving" CVE Talk at *TF-CSIRT Annual Group Meeting* on May 15
May 4, 2017

CVE Numbering Authorities Program Lead Dan Adinolfi will give a talk entitled "Expanding and Improving CVE to Facilitate Vulnerability Disclosure and Management" on May 15, 2017 at the *Task Force-Computer Security Incident Response Team (TF-CSIRT) Group Annual Meeting* in The Hague, the Netherlands.

Talk synopsis: "The Common Vulnerabilities and Exposures (CVE) program uniquely identifies and names publicly-disclosed vulnerabilities in software and other codebases. CVE Numbering Authorities (CNAs) are an important part of the CVE program and are given the ability to identify and name CVE IDs in coordination with the MITRE CVE team. Participating as a CVE CNA allows organizations to have more control over their vulnerability management and disclosure processes while also ensuring a consistent level of service and a high quality of content within the CVE list. Becoming a CNA can be beneficial to vendors, coordination centers, and their customers, and it helps build a community of practice that continues to help improve the state of vulnerability management across many sectors."

Visit the CVE Calendar for information on this and other events.

IOActive Added as CVE Numbering Authority (CNA)
April 25, 2017

IOActive is now a CVE Numbering Authority (CNA) for third-party products it researches.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 57 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; Canonical; CERT/CC; Check Point; Cisco; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Eclipse Foundation; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; IOActive; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Schneider Electric Added as CVE Numbering Authority (CNA)
April 20, 2017

Schneider Electric SE is now a CVE Numbering Authority (CNA) for Schneider Electric products only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 56 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; Canonical; CERT/CC; Check Point; Cisco; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Eclipse Foundation; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Schneider Electric; Siemens; Silicon Graphics; Symantec; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Minutes from CVE Board Teleconference Meeting on April 5 Now Available
April 20, 2017

The CVE Board held a teleconference meeting on April 5, 2017. Read the meeting minutes.

Eclipse Foundation Added as CVE Numbering Authority (CNA)
April 14, 2017

The Eclipse Foundation is now a CVE Numbering Authority (CNA) for Eclipse IDE and the Eclipse Foundation's eclipse.org, polarsys.org, and locationtech.org open source projects only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 55 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; Canonical; CERT/CC; Check Point; Cisco; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; Eclipse Foundation; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Siemens; Silicon Graphics; Symantec; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

"Expanding and Improving" CVE Talk at *SOURCE Boston 2017* on April 27
April 14, 2017

CVE Numbering Authorities Program Lead Dan Adinolfi will give a talk entitled Expanding and Improving CVE to Facilitate Vulnerability Disclosure and Management on April 27, 2017 at *SOURCE Boston 2017* in Boston, Massachusetts, USA. The event itself runs April 26-27.
From the event agenda:

"The Common Vulnerabilities and Exposures (CVE) program uniquely identifies and names publicly-disclosed vulnerabilities in software and other codebases. CVE Numbering Authorities (CNAs) are an important part of the CVE program and are given the ability to identify and name CVE IDs in coordination with the MITRE CVE team. Participating as a CVE CNA allows organizations to have more control over their vulnerability management and disclosure processes while also ensuring a consistent level of service and a high quality of content within the CVE list. Becoming a CNA can be beneficial to vendors, coordination centers, and their customers, and it helps build a community of practice that continues to help improve the state of vulnerability management across many sectors. Join Daniel Adinolfi of the CVE program to learn about these benefits and how to participate. Who should attend: CVE is a core piece of infrastructure that enables coordinated vulnerability disclosure and management. Developers, vulnerability researchers, product security incident response team (PSIRT) members, and anyone involved in vulnerability disclosure, research, or management processes would find value in attending."

To register for the event, visit http://www.sourceconference.com/boston-2017-registration.

Minutes from CVE Board Teleconference Meeting on March 22 Now Available
April 6, 2017

The CVE Board held a teleconference meeting on March 22, 2017. Read the meeting minutes.

Qualcomm Added as CVE Numbering Authority (CNA)
April 4, 2017

Qualcomm, Inc. is now a CVE Numbering Authority (CNA) for Qualcomm and Snapdragon issues only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 54 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; Canonical; CERT/CC; Check Point; Cisco; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Qualcomm; Rapid 7; Red Hat; Siemens; Silicon Graphics; Symantec; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Minutes from CVE Board Teleconference Meeting on March 8 Now Available
March 30, 2017

The CVE Board held a teleconference meeting on March 8, 2017. Read the meeting minutes.

Siemens Added as CVE Numbering Authority (CNA)
March 23, 2017

Siemens AG is now a CVE Numbering Authority (CNA) for Siemens issues only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 53 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; Canonical; CERT/CC; Check Point; Cisco; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Rapid 7; Red Hat; Siemens; Silicon Graphics; Symantec; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

FOCUS ON: The Significance and Meaning of a CVE Identifier Marked as "RESERVED"
March 16, 2017

A CVE Identifier (CVE ID) is marked as "RESERVED" when it has been reserved for use by a vendor or security researcher but the details of it are not yet populated by the requester.

A CVE ID can change from the RESERVED state to being populated at any time based on a number of factors both internal and external to MITRE.

An example of an internal factor could include the bulk assignment of CVE IDs to a CVE Numbering Authority (CNA). These CVE IDs are marked as RESERVED upon allocation to a CNA, before they are assigned to a specific vulnerability. An example of an external factor could include a vulnerability that have not yet been publicly disclosed, such as when the affected product vendor is still developing a mitigation.

It is also important to note that when a CVE ID is marked as RESERVED, it will not yet be available in the U.S. National Vulnerability Database (NVD). NVD is based-upon and fed by the CVE List.

However, once the CVE ID is populated with details and published on the CVE List on the CVE website, it will become available in NVD. As one of the final steps in the overall process, the NVD Common Vulnerability Scoring System (CVSS) scores for the CVE ID are assigned by the NIST NVD team.

Visit the FAQs page for answers to other questions about CVE IDs. You may also contact us with any comments or concerns.

CVE Launches "@CVEannounce" Twitter Feed
March 16, 2017

Please follow our second Twitter account at https://twitter.com/CVEannounce/ to get the latest CVE news and announcements.

Minutes from CVE Board Teleconference Meetings on February 8 and February 22 Now Available
March 16, 2017

The CVE Board held teleconference meetings on February 8, 2017 and February 22, 2017. Read the February 8 or February 22 meeting minutes.

Flexera Software and Netgear Added as CVE Numbering Authorities (CNAs)
March 14, 2017

Two additional organizations are now CVE Numbering Authorities (CNAs): Flexera Software LLC for all Flexera products and vulnerabilities discovered by Secunia Research that are not covered by another CNA, and Netgear, Inc. for Netgear issues only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 52 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; Canonical; CERT/CC; Check Point; Cisco; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; F5; Flexera Software; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Netgear; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Rapid 7; Red Hat; Silicon Graphics; Symantec; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Qihoo 360 Added as CVE Numbering Authority (CNA)
March 9, 2017

Qihoo 360 Technology Co., Ltd. is now a CVE Numbering Authority (CNA) for 360 Safeguard, 360 Mobile Safe, and 360 Safe Router issues only. CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 50 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; Canonical; CERT/CC; Check Point; Cisco; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; F5; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Qihoo 360; Rapid 7; Red Hat; Silicon Graphics; Symantec; Talos; TIBCO; VMware; and Yandex.
For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

CVE Launches New "CVE-CWE-CAPEC" Page on LinkedIn
March 9, 2017

The CVE Team has launched a "CVE-CWE-CAPEC page on LinkedIn" as an easy way for the community to comment on and share CVE Blog posts. Please stop by our new page and say hello. We very much look forward to hearing from you.

CVE Launches Twitter Feed of Newest CVE IDs
March 2, 2017

Please follow our new Twitter feed at https://twitter.com/CVEnew/ to get regular updates of the newest CVE IDs.

Drupal.org Added as CVE Numbering Authority (CNA)
February 28, 2017

Drupal.org is now a CVE Numbering Authority (CNA) for all issues for projects hosted under Drupal.org only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID. The following 49 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; Canonical; CERT/CC; Check Point; Cisco; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; Drupal.org; F5; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Rapid 7; Red Hat; Silicon Graphics; Symantec; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

"CVE-2005-4900" Is SHA-1 Collision Attack "SHAttered"
February 23, 2017

Researchers have published a practical method for crafting a file that shares a valid SHA-1 signature with another file. This vulnerability in SHA-1 was assigned CVE ID CVE-2005-4900 in 2016. The vulnerability described in this new research is the same as the vulnerability described in CVE-2005-4900, and this CVE ID can be used when referencing this vulnerability.

For more information on the results of this additional research, visit https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html or http://shattered.io/.

1 Product from Avatares Foundation Now Registered as Officially "CVE-Compatible"
February 23, 2017

One additional cyber security product has achieved the final stage of the CVE compatibility process and is now officially "CVE-Compatible." A total of 152 products to-date have been recognized as officially compatible

The following product is now registered as officially "CVE-Compatible":

Avatares Foundation	-	Pandora-CSF

To review all products and services listed, visit CVE-Compatible Products and Services.

Minutes from CVE Board Teleconference Meeting on January 25 Now Available
February 10, 2017

The CVE Board held a teleconference meeting on January 25, 2017. Read the meeting minutes.

Minutes from CVE Board Teleconference Meeting on January 11 Now Available
February 2, 2017

The CVE Board held a teleconference meeting on January 11, 2017. Read the meeting minutes.

New CVE Board Member from Black Duck Software
January 26, 2017

William Cox of Black Duck Software, Inc. has joined the CVE Board.

Read the full announcement and welcome message in the CVE Board email discussion list archive.

TIBCO Software Added as CVE Numbering Authority (CNA)
January 19, 2017

TIBCO Software, Inc. is now a CVE Numbering Authority (CNA) for TIBCO, Talarian, Spotfire, Data Synapse, Foresight, Kabira, Proginet, LogLogic, StreamBase, JasperSoft, and Mashery issues only.

CNAs are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities.

CNAs are the main method for requesting a CVE ID number. The following 48 organizations currently participate as CNAs: Adobe; Apache; Apple; BlackBerry; Brocade; Canonical; CERT/CC; Check Point; Cisco; Debian GNU/Linux; Dell EMC; Distributed Weakness Filing Project; F5; Fortinet; FreeBSD; Google; HackerOne; HP; Hewlett Packard Enterprise; Huawei; IBM; ICS-CERT; Intel; ISC; JPCERT/CC; Juniper; KrCERT/CC; Larry Cashdollar; Lenovo; MarkLogic; McAfee; Micro Focus; Microsoft; MITRE (primary CNA); Mozilla; Nvidia; Objective Development; OpenSSL; Oracle; Puppet; Rapid 7; Red Hat; Silicon Graphics; Symantec; Talos; TIBCO; VMware; and Yandex.

For more information about requesting CVE ID numbers from CNAs, visit Request a CVE ID.

Researcher Reservation Guidelines Document Now Available
January 12, 2017

The Researcher Reservation Guidelines document is now available on the CVE website. This document provides step-by-step guidelines on how to reserve a CVE ID(s) before publicizing a new vulnerability so that CVE IDs can be included in the initial public announcement of the vulnerability and can be used to track vulnerabilities.

CVE Updates Its Definition of "Vulnerability"
January 12, 2017

CVE has updated its definition of the term vulnerability as follows: "A 'vulnerability' is a weakness in the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that, when exploited, results in a negative impact to confidentiality, integrity, OR availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)."

Visit the Terminology page for additional information. You may also contact us with any comments or concerns.

FOCUS ON: The Significance and Meaning of the Year Portion of a CVE Identifier
January 12, 2017

CVE Identifiers (CVE IDs) have the format CVE-YYYY-NNNNN. The YYYY portion is the year that the CVE ID was assigned OR the year the vulnerability was made public (if before the CVE ID was assigned).

The year portion is not used to indicate when the vulnerability was discovered, but only when it was made public or assigned.

Examples:

- A vulnerability is discovered in 2016, and a CVE ID is requested for that vulnerability in 2016. The CVE ID would be of the form "CVE-2016-NNNN".
- A vulnerability is discovered in 2015 and made public in 2016. If the CVE ID is requested in 2016, the CVE ID would be of the form "CVE-2016-NNNNN".
- A vulnerability is discovered in 2015 and a request is made for a CVE ID in 2015. The vulnerability is assigned "CVE-2015-NNNN" but not made public. (The CVE ID would appear as "Reserved" in the CVE ID list.) The discloser does not publish the CVE ID publicly until 2017, though. In this case, the CVE ID is still "CVE-2015-NNNN", despite the fact that the vulnerability isn't made public until 2017.
- A vulnerability is discovered and published in 2015 without having a CVE ID assigned to it. Someone requests that a CVE ID be assigned to the vulnerability in 2016. The vulnerability is given "CVE-2015-XXXX" since it was first made public in 2015.

NOTE: Neither the date when a vulnerability was introduced into a product, or the date when a vulnerability was fixed in a product, factor into what year is indicated in the CVE ID assigned to that vulnerability.

Visit the FAQs page for answers to other questions about CVE IDs. You may also contact us with any comments or concerns.