CERN Computer Security

Computer security emergency contact
Computer.Security@cern.ch 70500
Contact en cas d'incident de sécurité informatique

Security Reports

Monthly reports on CERN security

CERN security statistics

Monthly security reports from SWITCH CERT

Articles & Announcements

Articles in the CERN Bulletin, Computing Newsletter & others

Announcement archive

SWITCH Security Blog

Conferences & Workshops

Presentations given by the Security Team

Trip reports from conferences

Theses & Reports

Theses of Security Team members

Reports of Security Team members

Computer Security Report for April 2019

An outdated Jenkins instance visible to the Internet has been compromized end of March. That instance has subsequently been used as a jump-host to scan the CERN office network for other vulnerable instances of Jenkins, Redis and probably other software (although we do not have any proofs for the latter). Indeed, two other Jenkins as a well as one Redis instances have been found compromised, too, with an automatic cronjob regularly pulling a Pastebin webpage for further instructions, and connecting to two particular domains for downloading the payload. Presumably, this was an automated attack with the intention to instantiate crypto-currency mining software (XMrig 2.14) on compromized hosts. All owners of local Jenkins instances are requested to check for those two processes: "kerberods" and "khugepageds". Please notify us at Computer.Security@cern.ch (mailto:Computer.Security@cern.ch) if you see hits. If you don't (and only if not), please upgrade your system to the newest version provided by either CERN OpenShift or directly from Jenkins.io. A more detailed advisory can be found here.

Related to the above, and for those who run Atlassian tools: Two critical "WebDAV and Widget Connector" vulnerabilities have been identified in the Confluence Server and Confluence Data Center (CVE-2019-3395 & CVE-2019-3396). Later, also a "Path traversal vulnerability" was reported (CVE-2019-3398). Several European and US sites were hit hard as was one CERN instance visible to the Internet. As this instance was not using CERN Single Sign-On, 53 users who logged into that instance after its compromise were requested to change their CERN password asap. Service managers running those tools should upgrade to the most recent versions.

A personal secret API key to a CERN-hosted conference management system has been found on the CERN Gitlab instance. Given that this API key was publicly visible to all CERN, anyone abusing that key would have had same access rights, and hence access to the same events and documents, as the owner of that key. However, no abuse has been detected. The key was revoked and the corresponding API functionality is currently being reviewed.

A new Apache vulnerability has been published recently. While not all versions are affected, users of Apache should check their deployments and should upgrade their installation to version 2.4.39 or above if necessary.

For Drupal, two moderately critical vulnerabilities were released for Drupal 8 and for Drupal 7 and 8. Please update you local Drupal instances, or migrate to the centrally managed Drupal service of the IT department.

And for those who run WAGO 750-xxx modules, please take notice that those devices provide an undocumented service access using hard-coded credentials which allow to change the settings of that module. if you can, please update your device to the latest firmware.

Due a to a misconfigured server, user email addresses and passwords of the scientific journal publisher "Elsevier" have been publicly exposed. The impacted users include people from universities and educational institutions from across the world, including 366 of CERN. While Elsevier insisted having informed all affected individual CERN users, we strongly suggest that owners of an account with Elsevier change their password now (if not already done during the past two weeks).

Our visit to a recent invitation-only underground security conference has been very

fruitful for CERN. Not only have we had very constructive discussions with renown security experts and specialist, but we could also secure a list of about 3000 passwords of which 561 were linked to valid CERN accounts and currently shared on the Dark Web among cyber-criminals. All affected account owners have been notified and asked to change their passwords ASAP.

In good tradition, more external passwords were lost by people having registered to external web services using their CERN email address: In January 2017, the data science website DataCamp suffered a data breach. The incident exposed 760k unique email and IP addresses along with names and passwords stored as bcrypt hashes. In October 2018, the Polish e-commerce website Morele.net suffered a data breach. The incident exposed almost 2.5 million unique email addresses alongside phone numbers, names and passwords stored as md5crypt hashes. All data sets appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. About ten affected people owning a CERN email adress have been notified.

The Wikis of any "CERN" software project on Github have all been found editable by any registered Github user. While no damage was done, all those Wikis were now restricted in access thanks to the quick intervention of the person responsible for github.com/CERN.

Mid-April, the Computer Security Team ran a very successful workshop on BroIDS/Zeek and MISP. The events have been completely booked out and the IT amphitheatre was packed for four days. Security professionals from four continents working in academia or private companies attended the events.

Threat Landscape for the Academic Community

This month has seen a severe attack affecting more than a dozen organisations and national labs in the US and Europe, including CERN (see above) and EGI/EOSChub. This attack is coming from the Chinese "Rocke Group", who aims at crypto-jacking, and probably others. Initially, the attackers were exploiting unpatched Jenkins and Redis systems, but changed recently their tactics and started to target Confluence applications. A more detailed advisory can be found here.

Recent articles on computer security

- "I love you"
- SWITCH's bimonthly security report

Statistics

Policy violations	
0	Copyright violations
9	SMTP
Interventions	
4	Device(s) compromized
1	Account(s) compromized
12	Webpage(s) found vulnerable
11	Jenkins/Redis; Confluence; API key; Apache; Drupal; WAGO; Elsevier; DarkNet; exposed passwords; Github Wikis; Bro/Zeek/MISP workshop

e-mail: **Computer.Security@cern.ch**
Phone: +41 22 767 0500
(Please listen to the recorded instructions.)

Please use the following PGP key to encrypt messages sent to
CERN Computer Security Team <**Computer.Security@cern.ch**>
429D 6046 0EBE 8006 B04C DF02 954C E234 B4C6 ED84