NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

November 2020, Edition 2.0

NETWORK INTELLIGENCE SECURITY ADVISORY

The major security news items of the month - major threats and security patch advisory. The advisory also includes IOCs and remediation steps.

IN THIS EDITION:

Security Advisory Listing	Severity
Remote Code Execution vulnerabilities (CVE-2020-28949, and CVE-2020-28948) within PEAR Archive_Tar library of Drupal which were widely exploited in Hacking Campaign and Malware distribution	Critical
Critical Remote code execution Vulnerability (CVE-2020-13671) was found in Critical Drupal platform – Government and Business entities were at high risk	Critical
Directory Traversal and Remote Code Execution Vulnerability (CVE- 2020-8271) in Citrix SD-WAN Center which was widely exploited in targeted hacking campaigns	Critical
A Threat Actor Group was found targeting Organisations IT systems using new ransomware called Egregor	Critical

ALSO INSIDE

Security Patch Advisory

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Remote Code Execution vulnerabilities (CVE-2020-28949, and CVE-2020-28948) within PEAR Archive_Tar library of Drupal which were widely exploited in Hacking Campaign and Malware distribution

Severity: Critical

Date: November 28, 2020

IMPACT

These vulnerabilities pose a severe risk of unauthorized access, data breach, data loss, interruption of business operation, impact reputation of an organization, and financial loss

REMEDIATION

1. Update Drupal 9.0.x, to version 9.0.9

2. Update Drupal 8.9.x, to version 8.9.10

3. Update Drupal 8.8.x or earlier, to version 8.8.12

4. Update Drupal 7, to version 7.75

5. Upgrade Drupal 8 prior to 8.8.x, to either of these versions 8.8.12, 8.9.10 or 9.0.9.

INTRODUCTION

Remote Code Execution vulnerabilities (CVE-2020-28949, and CVE-2020-28948) within PEAR Archive_Tar library of Drupal, is widely exploited in Hacking Campaign and Malware distribution.

These vulnerabilities is due to the PEAR Archive_Tar library improperly handle the file upload and processing functions when affected versions of Drupal is configured to allow uploading file with extensions such as .tar, .tar.gz, .bz2, .tlz, and triggers remote code execution while process the file.

In attack scenario, the remote attacker can take advantage of these vulnerabilities by uploading specifically crafted malicious file bearing extensions such as .tar, .tar.gz, .bz2, .tlz, and the moment Drupal site running affected version attempts to process the file, then it will trigger the code execution flaw to execute the malicious code on the Drupal site hosting server. As a result, it will allow remote attackers to gain unauthorized initial access to the Drupal site, and upload their malware for further distribution. Such vulnerabilities are often taken advantaged for malware distribution including Sodinokibi Ransomware attack.

These vulnerabilities pose a severe risk of unauthorized access, data breach, data loss, interruption of business operation, impact reputation of an organization, and financial loss.

AFFECTED PRODUCTS

- Drupal 9.0, versions prior to Drupal 9.0.9
- Drupal 8.9, versions prior to Drupal 8.9.10
- Drupal 8.8 or earlier, versions prior to Drupal 8.8.12
- Drupal 7, versions prior to Drupal 7.75

- Important:- Versions of Drupal 8 prior to 8.8.x are end-of-life and do notreceive security coverage.

READ

- Drupal core - Critical - Arbitrary PHP code execution - SA-CORE-2020-013

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Critical Remote code execution Vulnerability (CVE-2020-13671) was found in Critical Drupal platform – Government and Business entities were at high risk

Severity: Critical

Date: November 19, 2020

IMPACT

Successful exploitation of vulnerability (CVE-2020-13671) in Drupal platform, poses a risk of unauthorized access, data breach, interruption of services, privilege escalation and impact reputation of an organization

REMEDIATION

1. Kindly update Drupal 9.0 to Drupal 9.0.8
2. Kindly update Drupal 8.9 to Drupal 8.9.9
3. Kindly update Drupal 8.8 or earlier to Drupal 8.8.11
4. Kindly update Drupal 7 to Drupal 7.74

5. Ensure no unauthorized system changes have occurred before applying patches.

6. Run all software as a non-privileged user to diminish effects of a successful attack.

7. Apply the Principle of Least Privilege to all systems and services.

TEMPORARY MITIGATION

Disable all web services modules or configure your web server(s) to not allow GET/PUT/PATCH/POST requests to web services resources.

INTRODUCTION

A vulnerability has been discovered in the Drupal core module, which could allow for remote code execution. Drupal is an open source content management system (CMS) written in PHP. Successful exploitation of this vulnerability could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

The remote code execution vulnerability exists due to a lack of proper data sanitization of certain filenames on uploaded files. This can lead to files being interpreted as the incorrect extension, served as the wrong MIME type, or executed as PHP for certain hosting configurations.

AFFECTED PRODUCTS

- Drupal Core versions prior to 9.0.8, 8.9.9, 8.8.11, and 7.74

READ

- Drupal core - Critical - Remote code execution - SA-CORE-2020-012
- Remote Code Execution Vulnerability Patched in Drupal

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Directory Traversal and Remote Code Execution Vulnerability (CVE-2020-8271) in Citrix SD-WAN Center which was widely exploited in targeted hacking campaigns

Severity: Critical

Date: November 18, 2020

IMPACT

Successful exploitation of these vulnerabilities (CVE-2020-8271, CVE-2020-8272, CVE-2020-8273) in Citrix SD-WAN Center, poses a risks of unauthorized access, data breach, interruption in business services, cause financial loss, and impact reputation of an organization.

REMEDIATION

1. Kindly update Citrix SD-WAN 11.2.x, to version 11.2.2 and later
2. Kindly update Citrix SD-WAN 11.1.x, to version 11.1.2b and later
3. Kindly update Citrix SD-WAN 10.2.x, to version 10.2.8 and later.

INTRODUCTION

Directory Traversal and Remote Code Execution Vulnerability (CVE-2020-8271) in Citrix SD-WAN Center, is widely exploited in targeted hacking campaigns.

The unauthenticated remote attackers are taking advantage of this vulnerability (CVE-2020-8271) to gain unauthorized access onto the restricted directory path and perform unauthorized API operations on files stored on the affected Citrix SD-WAN Server, by sending a specifically crafted packets.

The unauthenticated remote attackers can also take advantage of Authentication Bypass Vulnerability (CVE-2020-8272) to gain unauthorized access to any Citrix SD-WAN API interface, and further exploit Privilege Escalation Vulnerability (CVE-2020-8273) to execute arbitrary commands as Root, by sending a specifically crafted packets.

Successful exploitation of these vulnerabilities (CVE-2020-8271, CVE-2020-8272, CVE-2020-8273) in Citrix SD-WAN Center, poses a risks of unauthorized access, data breach, interruption in business services, cause financial loss, and impact reputation of an organization.

These risks can be temporarily mitigated either by limiting exposure of or restricting access to Citrix SD-WAN Center (which is an internal management platform for Citrix SD-WAN) from internet and DMZ facing sides. However, it is strongly recommended to apply available security patches to completely mitigate the risks.

AFFECTED PRODUCTS

- Citrix SD-WAN 11.2.x before 11.2.2
- Citrix SD-WAN 11.1.x before 11.1.2b
- Citrix SD-WAN 10.2.x before 10.2.8

READ

- Citrix SDWAN Center Security Update
- SD-PWN Part 2 — Citrix SD-WAN Center — Another Network Takeover

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A Threat Actor Group was found targeting Organisations IT systems using new ransomware called Egregor

Severity: Critical

Date: November 16, 2020

IP SUBNETS

49.12.104.241
91.199.212.52

REMEDIATION

1. Block the threat indicators at their respective controls.
2. Do not download untrusted email attachments coming from unknown email addresses.
3. Keep all systems and software updated to latest patched versions

READ

- Rewterz Threat Alert – Egregor Ransomware – Continued Malicious Activities
- Egregor Ransomware Threatens 'Mass-Media' Release of Corporate Data
- CERT-In is warning companies in India to be careful about a new ransomware
- Egregor ransomware gang leaked data alleged stolen from Ubisoft, Crytek

HASH (SHA-256)

Hashes	DETECTEDBYANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
c94fdfedd40e0b194165294f48497794 7df9da2000cb8fe02243961384b249ff	Yes	Yes	yes	Yes	Yes
7d587a5f6f36a74dcfbcbaecb2b0547fdf 1ecdb034341f4cc7ae489f5b57a11d	Yes	Yes	Yes	No	Yes
3c2fe308c0a563e06263bbacf793bbe9b 2259d795fcc36b953793a7e499e7f71	Yes	Yes	yes	No	Yes
14296b21c6e2ba9d56759e2da4b09f58 148852ddeefa8fb76a838a30871679a7	Yes	Yes	Yes	Yes	Yes
14296b21c6e2ba9d56759e2da4b09f58 148852ddeefa8fb76a838a30871679a7	Yes	Yes	Yes	Yes	Yes
14296b21c6e2ba9d56759e2da4b09f58 148852ddeefa8fb76a838a30871679a7	Yes	Yes	Yes	Yes	Yes
14296b21c6e2ba9d56759e2da4b09f58 148852ddeefa8fb76a838a30871679a7	Yes	Yes	Yes	Yes	Yes
14296b21c6e2ba9d56759e2da4b09f58 148852ddeefa8fb76a838a30871679a7	Yes	Yes	Yes	Yes	Yes
14296b21c6e2ba9d56759e2da4b09f58 148852ddeefa8fb76a838a30871679a7	Yes	Yes	Yes	Yes	Yes
14296b21c6e2ba9d56759e2da4b09f58 148852ddeefa8fb76a838a30871679a7	Yes	Yes	Yes	Yes	Yes
14296b21c6e2ba9d56759e2da4b09f58 148852ddeefa8fb76a838a30871679a7	Yes	Yes	Yes	Yes	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

NEWSLETTER

November 2020, Edition 2.0

DATA BREACH HIGHLIGHTS

BigBasket, an Indian-based online grocery store had suffered data breach incident that exposed 20 million user records to cyber criminals on underground forum

November 29, 2020

- 20 million Bigbasket user records available on the dark web
- Bigbasket faces potential data breach

Belden, the manufacturer of networking and cable products had suffered data breach incident caused by threat actors

November 26, 2020

- Belden discloses data breach as a result of cyber attack

The North Face, an American outdoor recreation product company had suffered a credential stuffing attack followed by data breach incident caused by attackers

November 15, 2020

- The North Face website suffered a credential stuffing attack